The University of Jordan

Authorization Form

I, Maha K. Saadeh, authorize the University of Jordan to supply copies of my Thesis/ Dissertation to libraries or establishments or individuals on request, according to the University of Jordan regulations.

Signature: Saadeh

Date: 9-8-2011

الجامعة الأردنيـــة
كلية الدراسات العليا

التاريـــخ: / /

نموذج رقم (١٨)
اقرار والتزام بالمعايير الأخلاقية والأمانة العلمية
وقوانين الجامعة الأردنية وأنظمتها وتعليماتها
لطلبة الماجستير

أنا الطالب: مها خالد محمد سعاده الرقم الجامعي: (٨٠٩٠١٠٩)

تخصص: ماجستير علم الحاسوب الكليــــــة: الملك عبدالله الثاني لتكنولوجيا المعلومات

عنوان الرسالة: Secure Routing Protocol for Wireless Sensor Networks

اعلن بأنني قد التزمت بقوانين الجامعة الأردنية وأنظمتها وتعليماتها وقراراتها السارية المفعول المتعلقة باعداد رسائل الماجستير عندما قمت شخصيا" باعداد رسالتي وذلك بما ينسجم مع الأمانة العلمية وكافة المعايير الأخلاقية المتعارف عليها في كتابة الرسائل العلمية. كما أنني أعلن بأن رسالتي هذه غير منقولة أو مستلة من رسائل أو كتب أو أبحاث أو أي منشورات علمية تم نشرها أو تخزينها في أي وسيلة اعلامية، وتأسيسا" على ما تقدم فانني أتحمل المسؤولية بأنواعها كافة فيما لو تبين غير ذلك بما فيه حق مجلس العمداء في الجامعة الأردنية بالغاء قرار منحي الدرجة العلمية التي حصلت عليها وسحب شهادة التخرج مني بعد صدورها دون أن يكون لي أي حق في التظلم أو الاعتراض أو الطعن بأي صورة كانت في القرار الصادر عن مجلس العمداء بهذا الصدد.

توقيع الطالب: Saadeh التاريخ: ٩ / ٨ / ٢٠١١

SECURE ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

By

Maha Khaled Saadeh

Supervisor

Dr. Iman Almomani

This Thesis was Submitted in Partial Fulfillment of the Requirements for the Master's Degree of Science in Computer Science

Faculty of Graduate Studies

The University of Jordan

August, 2011

This Thesis/ Dissertation (Secure Routing Protocol for Wireless Sensor Networks) was Successfully Defended and Approved on 28-7-2011

Examination Committee	**Signature**
Dr. Iman M. Almomani, Supervisor Assist. Prof. of Wireless Networks and Network Security.	------------------------------
Dr. Saleh H. Sharaeh, Member Prof. of Parallel, Distributed and Mobile Computing	------------------------------
Dr. Basel A. Mahafzah, Member Assoc. Prof. of Distributed and Parallel Computing, and Interconnection Networks	------------------------------
Dr. Jehad A. Al-Sadi, Member Assoc. Prof. of Interconnection Networks Arab Open University, Amman	------------------------------

DEDICATION

To My Wonderful Parents,

Sisters and Brother,

And

To All My Friends and Colleagues

Maha Saadeh

ACKNOWLEDGEMENT

First and foremost I want to thank "Allah" for giving me the strength, wisdom, hope and knowledge to share this work with others and for that many talents and blessing that he has blessed me with.

I would like to acknowledge my beloved supervisor, Dr. Iman Almomani for her great support and the effort that she has been giving me.

Also I want to thank my parents, brother, and sisters for their endless patience, encouragement, and love.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVIATION	MEANING
AES	Advanced Encryption Standard
AODV	Adhoc On demand Distance Vector
BS	Base Station
CBC-MAC	Cipher Block Chaining-Message Authentication Code
C_{max}	maximum number of Children
DS	Digital Signature
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ETR	Enhance Tree Routing
FEAR	Fuzzy Energy Awareness Routing
GAF	Geographic Adaptive Fidelity
ID	Identifier
IDS	Intrusion Detection System
ImpTR	Improve Tree Routing
LEACH	Low Energy Adaptive Clustering Hierarchy
MAC	Message Authentication Code
PKC	Public Key Cryptography
QoS	Quality of Service
SPIN	Sensor Protocol for Information via Negotiation
TR	Tree Routing

SECURE ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

By
Maha Khaled Saadeh

Supervisor
Dr.Iman Al-momani

ABSTRACT

Recently, Wireless Sensor Networks (WSNs) are considered as an important topic that received a significant interest by many researchers. This interest comes from the successful use of sensor technology in many civilian, military, and industrial applications. Resource limitation and wireless network characteristics are the main challenges facing the development and deployment of WSN protocols. Any protocol that is proposed for WSN should consider its low power and limited processing and storage capabilities. In addition, the researchers should consider the unreliable and unsecure wireless links while routing the data between network nodes.

Many routing protocols have been proposed for WSNs. Some of these protocols take the limited power of the sensor network in their considerations, while the others do not. In this thesis, a resource efficient routing protocol, called Fuzzy-based Energy Aware Routing (FEAR) protocol, is improved by applying some security mechanisms to build an energy efficient secure routing protocol that protects the network from different types of security attacks. The main idea is to evaluate the protocol before and after applying security mechanisms to assess the impact of attackers on the network topology and routing process. In addition, the cost of achieving security requirement based on symmetric and asymmetric security approaches will be measured.

QualNet 5.0 network simulator is used to evaluate the routing protocol. Cipher Block Chaining-Message Authentication Code (CBC-MAC) and Elliptic Curve Digital Signature Algorithm (ECDSA) are two well-known security schemes that are used in this thesis to achieve authentication and data integrity based on symmetric and asymmetric approaches respectively. The results show that considering only the resource limitations for sensor nodes is not enough to develop an efficient routing protocol without protecting the network from different routing attacks since attackers can drop network power over the time.

After applying the security schemes, the results reveal that despite of the percentage of attackers, achieving authentication and data integrity will exclude them all from the network topology. Consequently, the constructed topology will be secure and can be used for safe data transmission. Moreover, the simulation results reveal that using CBC-MAC will cost 0.00064 % of network power and using ECDSA costs about 0.0091 %. Although this cost is required to achieve the needed security requirements, the results illustrate that some attackers will cost the network about 4.7 times the cost of achieving these requirements.

Chapter One

Introduction

1.1 Motivation

Recently, the importance of Wireless Sensor Networks (WSNs) has been increased due to the successful use of sensor technology in different military, civilian, and industrial applications (Biradar, et al., 2009) (Jamalipour, et al., 2009). This type of wireless networks consists of small size, low cost, and low power sensor nodes. Each sensor has processing and communication capabilities in a company with sensing facility (Jamalipour, et al., 2009) (Al- karaki, et al., 2004).

Different uses of WSNs can be found in medical, military, and industrial fields. In the field of medical and healthcare, WSNs are widely used to monitor patients and record their status. Patients' data is sent to the base station, which is usually called the sink node, by different sensors placed on patient's body or his surrounding environment. This data is used to follow patient's conditions in his own home. This out-of-hospital treatment does not replace the role of hospitals and healthcare centres; instead, it involves the patients to be active participants in their own healthcare. (McGrath, et al., 2010) (Jamalipour, et al., 2009).

In military applications, WSNs have important role as well. They can be used in battlefield monitoring, intelligent guiding, and detecting enemies' attacks. Moreover, the applications of WSNs can be found in environmental monitoring, disaster relief, emergency rescue operation, product quality monitoring, and many other applications. (Biradar, et al., 2009).

Some of WSNs applications require secure data transmission. In such applications different security defense schemes should be applied to ensure authorized

data access, confidential data transmission, and achieving data integrity. On the other hand, some applications require high reliability and bounded delivery time. The protocol designed for these applications should consider routing issues such as shortest path discovery, multi-node to node routing, and the use of multiple sinks to increase network availability and reliability.

Generally, it is important to design and implement resource-efficient routing protocols that will transmit the data while considering nodes resource limitation and try to give best power saving. Also, it is important to apply an efficient security framework to protect both sensor nodes and network topology from different routing attacks. Thus, bearing in mind both resource limitations and routing threats while developing routing protocols will prolong network life time and increase its availability and reliability.

1.2 Problem Definition

Many challenges face the design and implementation of WSNs. One important challenge is the limited resources of sensor devices. Unlike other devices such as PC and PDA, sensors are resource constraints devices that suffer from small computational and communicational capabilities, limited memory storage, and limited amount of power (Al- karaki, et al., 2004) (Biradar, et al., 2009) (Jamalipour, et al., 2009).

In addition to resource limitations, the characteristics of wireless communication present additional challenges in the design of WSN protocols (Jamalipour, et al., 2009). The use of unreliable and unsecure wireless links requires reliable routing solutions and secure data transmission.

For routing protocols the challenge is to route the message using suitable path and at the same time try to prolong network life time by avoiding excessive messages that are exchanged between nodes, thus, reducing the overall consumed power. On the other hand, applying well defined security framework will protect the network from different attacks. Consequently, network availability will be increased.

Recently, due to the significant use of WSN in many sensitive applications such as healthcare and military applications, maintaining data security becomes a major challenge in the implementation of WSNs protocols. In such applications, the correctness of the important, sensed data is affected as less security requirements achieved. Thus it is important to consider security issues and possible threats in any protocol design. In fact breaking data security not only diminishes its importance but also affects the application objectives by providing false alarms and wrong reactions.

1.3 Contribution

As mentioned in the previous sections, it is important to use resource-efficient routing protocols and well defined security architecture to transmit and process the data in a secure manner. In the literature there are many routing protocols proposed for WSNs. These protocols consider routing issues with or without considering sensors power limitation or possible network threats. In this thesis, we will improve a power efficient tree-based routing protocol, called the FEAR protocol (ALmomani, et al., 2011), by applying different security mechanisms to show that considering only the resource limitations for sensor nodes is not enough to develop an efficient routing protocol without protecting the network against different routing attacks. The main idea is to evaluate the FEAR protocol before and after applying the selected security

mechanisms to assess the impact of attackers on network topology and routing process. In addition, measure the cost of achieving some security requirements such as nodes authentication and data integrity by applying different security mechanisms on the FEAR protocol.

1.4 Thesis Organization

Chapter two introduces a background on sensor networks, routing protocols, and security issues. Moreover, it summarizes some related works from the literature. Chapter three discusses the possible routing attacks and how to apply security mechanisms to secure the network from these attacks. In chapter four we present the evaluation and simulation results. Finally, chapter five concludes the thesis and presents the future work.

Chapter Two
Literature Review

2.1 Background

In this section a background on WSNs, routing protocols, and security issues will be discussed.

2.1.1 Wireless Sensor Networks (WSNs)

Wireless Sensor Networks (WSNs) are infrastructure-based networks that consist of small sensors scattered in the sensing environment and one or more sink node(s). Sensors are resource constraints devices; they have limited computational capabilities, small memory storage, and finite battery. They are used to sense environmental data and send it to the sink (Al- karaki, et al., 2004). The sink node is used to process sensed data and connect the sensor network to the Internet or other wired networks. Unlike sensors, sink node is a powerful device that is connected to a power supply. Figure 1 shows an example of WSN.

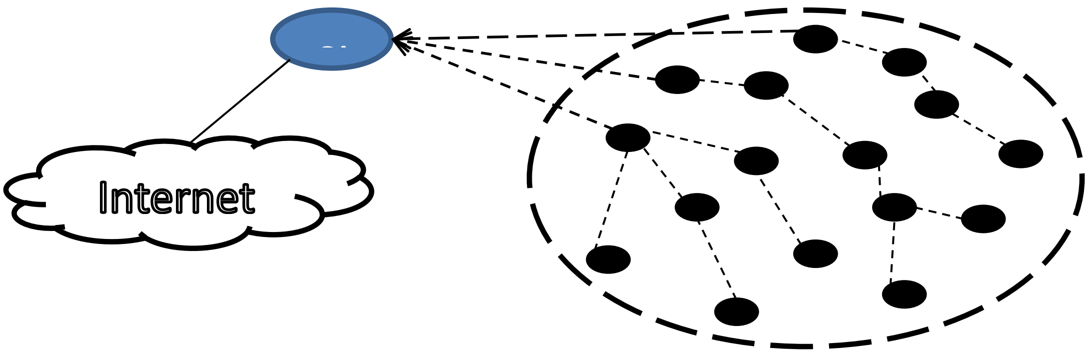


Figure 1: Example of wireless sensor network.

Each sensor is embedded with a microprocessor and a wireless transceiver along with the sensory unit providing data processing and communication capabilities in a company with sensing facility. Figure 2 shows the main components of sensor device

which are: microcontroller for data processing, local memory, sensor for data collection, analog-to-digital converter (ADC) for signal conversion, transceiver for wireless communication, and power supply unit.

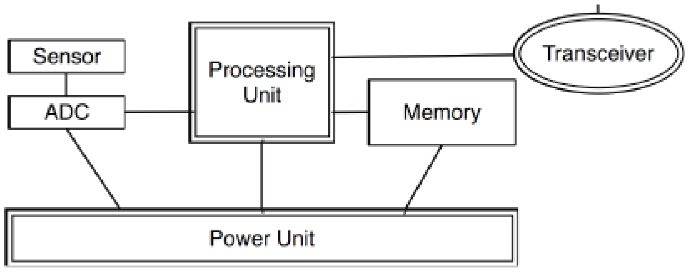


Figure 2: Sensor components (Neves, et al., 2008).

MicaZ and TolesB are two known sensor motes differ in their memory size and energy efficiency. MicaZ motes have 4 KB of RAM, 128 KB of ROM and TelosB motes have 10 KB of RAM, 48 KB ROM. Regarding energy efficiency TolesB motes are more efficient than MicaZ (Lee, et al., 2010).

2.1.2 The Classification of Routing Protocols in WSNs

Many protocols have been proposed for WSNs. These protocols are classified according to network structure, protocol operation, and route discovery (Al- karaki, et al., 2004). Figure3 illustrates these classifications. According to network structure, protocols are divided into flat, hierarchical, and location based protocols. In flat network routing protocols, all nodes play the same role and sensors collaborate to perform the sensing task. Since there are a large number of nodes in such networks, it is not feasible to assign a global identifier to each node. This type of routing called data-centric routing in which the BS sends queries to a selected region and waits for data from the sensors located in that regions. Query based process requires an attribute-based naming to

specify the properties of data in order to eliminate redundant data and save energy (Akkaya, et al., 2005).

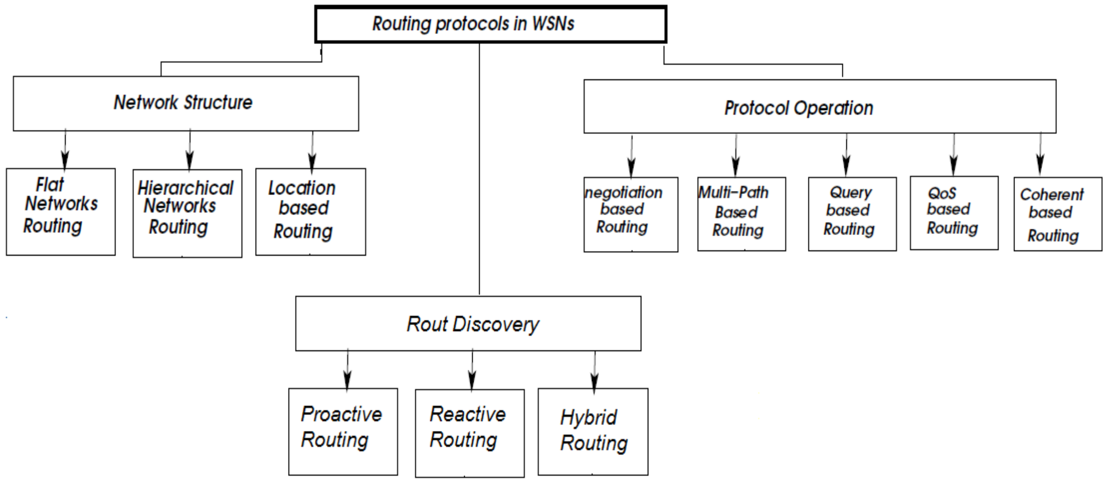


Figure 3: Routing protocols classification.

One protocol based on data centric routing is the SPIN (Sensor Protocols for Information via Negotiation) (Kulik, et al., 2002). The main goals behind the SPIN are to eliminate redundant information passing and overlapping of sensing areas caused by flooding protocols, thus, achieving better energy efficiency. The idea is to name the data using high-level descriptors or meta-data. For each new data, the corresponding meta data should be exchanged among sensors. This process is called advertisement process since nodes advertise the new data to their neighbors and only interested neighbors will send a request message to retrieve the data. The drawback of SPIN protocol is that data advertisement mechanism cannot guarantee the delivery of data. This occurs when the nodes that are interested in the data are far away from the source node and all nodes between them are not interested in that data.

Other protocols utilize the concept of hierarchical routing to perform energy-efficient routing in WSNs and achieve better system lifetime. In these protocols higher-energy nodes can be used to process and send the information, while low-energy nodes can be used to perform the sensing (Akkaya, et al., 2005). One well known hierarchical protocol is the LEACH (Low-Energy Adaptive Clustering Hierarchy) (Heinzelman, et al., 2000). The idea is to divide the network into clusters and choose a cluster head for each one. All local cluster heads will be used as routers to the sink. This clustering will save energy since all the data is processed locally inside the cluster. Moreover, the transmissions will be done through cluster heads rather than involving all sensor nodes. Cluster heads are changed randomly over time in order to balance the energy dissipation of nodes. However, LEACH is not applicable to networks deployed in large regions, since it uses single-hop routing where each node can transmit the data directly to the cluster head. Furthermore, the idea of dynamic clustering brings extra overhead, which may diminish the gain in energy consumption.

Another cluster head routing algorithm is proposed in (Zhang, et al., 2008). The network is divided into clusters. In each cluster, the node that has the maximum power is selected to be a cluster head. The cluster head is used for intra-cluster data gathering and inter-cluster communication. The authors use the principle of Prim and Djkstra to build a shortest routing tree algorithm. This algorithm is used in the inter-cluster communication to transmit the data to the sink node. The cluster heads are changed in turn to balance the energy among network nodes. To reduce network power consumption an energy-prediction model based on markov chains is proposed. Each node predicts its future energy according to its past history. Instead of sending frequent messages to refresh nodes available energy, nodes need to send one message including

their available energy and the required parameter to describe their energy dissipation. The drawback of this algorithm is the overhead of prediction operations and clustering process.

Other protocols such as Geographic Adaptive Fidelity (GAF) (Xu, et al., 2001) are based on nodes location. In this type of protocols, sensor nodes are addressed by means of their locations. In most cases location information is needed to estimate energy consumption by calculating the distance between two particular nodes. This distance can be estimated according to incoming signal strengths (Al- karaki, et al., 2004). If the region to be sensed is known then queries can be diffused only to that particular region which consumed less energy. More energy can be saved by using power management schemes. In GAF each node uses its GPS to associate itself with a point in a virtual grid. All nodes that are associated with the same point on the grid are considered equivalent in terms of packet routing cost. This can be used to save network energy by keeping equivalent nodes in sleeping state. Sleeping nodes change to active state in turn to balance the load between nodes. The drawback in location based protocols is that the region where the destination is located must be known before sending the queries.

According to network operations protocols are divided into negotiation based, multipath based, QoS based, query based, and coherent based routing protocols (Al-karaki, et al., 2004). Negotiation based protocols are data centric protocols. SPIN protocol (discussed previously) is an example on this type of protocols.

Multipath routing protocols use multiple paths rather than a single path to transmit the data to the destination. This can be used to increase system reliability and availability at the expense of increasing energy consumption, overhead, and traffic generation (Stavroua, et al., 2010).

In Query-Based Routing the destination nodes propagate a query for data through the network. Each node with required data sends it back to the node that initiated the query (Akkaya, et al., 2005). Directed diffusion (Intanagonwiwat, et al., 2000) is an example of this type of routing. In directed diffusion the Base Station (BS) sends interest messages to sensors. The sensor that has the required data sends it back to the BS. For each interest, a path from the sensor back to the BS should be established in order to send the data of interest.

In QoS-based routing protocols, the network has to balance between energy consumption and data quality. The main idea is to satisfy certain QoS metrics when delivering data to the BS (Villalba, et al., 2009) (Biradar, et al., 2009). Sequential Assignment Routing (SAR) (Akyildiz, et al., 2002) is the first protocol for sensor networks that includes the notion of QoS in its routing decisions. It is a table-driven multi-path protocol aims to achieve energy efficiency and fault tolerance. It creates trees rooted at the source node. Multiple paths from sink to source sensors are formed considering different QoS metric and energy resource on each path. However, this protocol suffers from the overhead of maintaining the tables and states at each sensor especially in large networks.

Coherent and non-coherent based routing protocols concern with data processing on sensor nodes. In non-coherent routing nodes will locally process the raw data before sending it to aggregator nodes for further processing. In coherent routing, the data is forwarded to aggregators after minimum processing, consequently, a better energy-efficient routing is achieved (Al- karaki, et al., 2004).

According to route discovery the protocol can be a proactive, reactive, or hybrid between them. Reactive protocols find a route on demand by flooding the network with route request packets. The advantage of this type of protocols is that it does not have to keep routing information to all nodes. The main disadvantages are high latency time in route finding and overhead of excessive flooding (Jung, et al., 2007). A well known example is AODV (Adhoc On demand Distance Vector) protocol (Perkins, et al., 1999). AODV tries to find the shortest route possible. When a node requires a route it initiates a route discovery procedure and broadcast Route REQuest (RREQ) messages. When receiving RREQ the node creates and sends a Route REPly (RREP) message back to the originator node if either it has a valid route entry to the destination or it is the destination itself. Every node maintains route entries with forward and backward next hop information along with its expiry time.

Unlike reactive protocols the proactive protocols maintain fresh lists of destinations and their routes by distributing routing tables throughout the network. The tables are updated either periodically or when changes are recognized. The main disadvantage is the overhead of maintaining and updating the routing tables. Hybrid protocols use a combination of these two ideas (Jung, et al., 2007).

2.1.3 Security Issues in WSNs

Securing the system against threats and attacks is one of the challenges facing the deployment of sensor network. Network attacks are mainly classified as internal or external attacks. In the former type the attacks are done by authenticated nodes. This type is dangerous since attacker can access network data and fake other nodes. To protect the network against internal attacks Intrusion Detection Systems (IDS) should be applied. These systems detect the compromised nodes and exclude them from the network.

External attackers are less dangerous than internal ones since they are unauthenticated nodes and they cannot access network data if suitable security prevention techniques are used. Prevention techniques include digital certificate, digital signature, encryption, Message Authentication Code (MAC) algorithms and others. The use of prevention technique depends on the security requirements that are needed to be achieved. Different security requirements should be considered to secure the system against security threats and attacks and the need of these requirements depends on the application itself. Table 1 lists these requirements and the prevention technique that are used to achieve them.

Table 1: Security Requirements and Security Enforcers.

Security Requirement	Meaning	Prevention Technique
Authorization	Give different privileges to network nodes.	Firewall
Authentication	Proof of identity	Digital Signature, Digital Certificate, MAC
Confidentiality	Data secrecy	Encryption

Data integrity	The data is received without any modification.	Digital Signature, MAC, Hashing
Non repudiation	The node cannot deny any operation.	Digital Signature

2.2 Related Work

Many routing protocols have been proposed for WSNs. In this section some of these protocols are discussed.

2.2.1 Tree-based Routing Protocols in WSN

Tree Routing (TR) protocol is a tree based protocol that is suitable for low power, low capabilities, and lightweight networks. This protocol is supported by IEEE802.15.4 (IEEE, 2005) and aims to reduce excessive messages and eliminate the overhead of path searching and updating. However, this protocol suffers from two drawbacks. First, message transmission depends on source depth; the deeper the node the longer the path. Second, it suffers from node/link failure that causes nodes isolation.

Many researches have been carried out trying to improve the performance of TR protocol. In (Jung, et al., 2007) Plus Tree routing protocol is proposed. This protocol constructs a tree between network nodes and uses neighbors table to store neighbors' information. Its main advantage is that it uses both parent-child links and neighbor links to transmit the message in the shortest path. In addition to that, Plus Tree protocol provides a solution to solve link failure problem. However, this protocol does not consider nodes energy in its solutions. In (Qiu, et al., 2009) and (Al-Harbawi, et al., 2009) Enhance Tree Routing (ETR) and ImpTR protocols are proposed for zigbee

network respictively. Both ETR and ImpTR trying to improve TR protocol by transmitting the packets over the shortest path to the sink node. Like plus tree protocol these protocols parent-child and neighbor links are used to find the shortest path to the sink, but they do not consider network energy.

In (Mohajerzadeh, et al., 2010) the authors propose an energy efficient tree based routing protocol which tries to manage congestion and to provide fairness in network. First the protocol divides the nodes into clusters then it constructs a routing tree for each cluster. This tree will be used for data transmission considering two traffic types; high priority and low priority. All nodes should build routing tables to be used in the data transmission phase. Keeping the information of these tables up to date is costly and increases the consumed power.

Fuzzy-based Energy Aware Routing (FEAR) protocol proposed in (ALmomani, et al., 2011) is a tree based routing protocol that aims to overcome the problems in TR protocol by providing energy efficient solutions to tree construction and node failure. To construct the tree between network nodes FEAR protocol uses fuzzy logic to rank the nodes according to specific parameters such as node power, node depth, and node distance from the sender. If the node has a high rank then it has a better chance to be selected as a parent. This will keep the balance between network nodes. The advantages of this protocol is that it reduces the overhead in the number of sent and received messaged between nodes. In addition it considers power limitation in its solutions. On the other hand FEAR protocol does not consider security issues in its implementation.

2.2.2 Secure Routing Protocols in WSN

All of the previous protocols consider only routing issues and how to transmit the data to the sink without considering possible attacks. In this section we will discuss some tree based secure routing protocols.

In (Abuhelaleh, et al., 2008) Armor LEACH protocol is proposed to secure the LEACH protocol by proposing authentication, confidentiality and integrity security mechanisms. The authors in (Mukesh, et al., 2009) (Kanjee, et al., 2010) (Dimitriou, et al., 2008) propose authentication and confidentiality solutions to be used for WSN. These papers use different network topologies and assume that routing issues are handled by the network layer. In (Mukesh, et al., 2009) (Kanjee, et al., 2010) the authors used biometric-based authentication scheme. In this scheme two or more sensors measure the same biometric and find a specific value. This value can be used as a shared key or sent to the sink node to perform the authentication process. One disadvantage of biometric-based authentication is that sensors must be synchronized in order to measure the value at the same time. Another disadvantage is that all sensors should measure the same biometric which is not always true. In (Dimitriou, et al., 2008) three security services are defined. These services are authentication, confidentiality, and replay attack protection. The authors utilize three bits in the TinyOS packet format to support the three services. Each bit is assigned to one service. When any service needs to be applied, the packet format should be modified to support the applied service. The disadvantage is that this technique is platform dependent and can only apply on sensors with TinyOs platform.

In (Söderlund, 2006) the author studied the impact of adding message authentication code on the life time of wireless sensor network based on different symmetric and asymmetric approaches. The results show that the lifetime of a sensor node is almost not affected by the addition of authentication. In addition, the results show that using symmetric based authentication is more efficient that asymmetric approaches. However, this work does not consider energy factor in its comparisons.

In (Pathan, et al., 2007) the authors proposed a secured routing for tree based networks by ensuring authentication and confidentiality using one way hash chain and preloaded key. A sink rooted tree is constructed to be used in the routing process. To ensure authenticity of the transmitted data, all the intermediate nodes must be initialized with the basic one-way hash chain number during the tree construction. The authors assume that no node could be compromised during the tree construction.

Another secure protocol for tree based routing is proposed in (Papadimitriou, et al., 2009). This protocol uses Public Key Cryptography (PKC) to protect the network against sinkhole attacks by sign the message to prove its identity. In (Ren, et al., 2007) and (Yeh, et al., 2011) the authors presented authentication schemes based on PKC. In (Ren, et al., 2007) the authors used different cryptographic techniques, such as Merkle hash tree and identity-based signature schemes, to achieve immediate broadcast authentication and to minimize the computation and communication cost. The authors in (Yeh, et al., 2011) provided an Elliptic Curve Cryptography (ECC) based solution to achieve authentication. Another ECC authentication scheme is proposed in (Gupta, et al., 2010). The main disadvantage in these protocols is that PKC is not efficient to be used in WSNs due to its complexity and its high power requirement.

In this thesis, we will focus on improving the energy efficient tree based routing protocols in WSNs by applying security schemes to ensure constructing a secure topology among network nodes. Consequently this topology will be used for safe data transmission. FEAR protocol has been chosen due to its efficiency in solving the problems of TR and other tree based protocols in terms of reducing the number of messages that are exchanged between network nodes. In addition, it provides power efficient solutions to solve node(s)/link(s) failure problem. By applying energy efficient security schemes to FEAR protocol we will build a well-structured secure routing protocol to protect the network against different threats and attacks.

Chapter Three

Attacks Model Evaluation and Security Solutions

This chapter discusses the possible attacks in FEAR protocol and how they affect the tree construction among network nodes. In addition, it will also discuss how to improve FEAR protocol by applying some security mechanisms to build an energy efficient secure routing protocol that protects the network against security attacks.

3.1 FEAR Overview

FEAR (ALmomani, et al., 2011) is a tree based routing protocol that aims to improve the TR by allowing the use of neighbors' links to forward the data packet and providing power efficient solution to link(s)/node(s) failure. As TR protocol, FEAR reduces excessive control messages between nodes and eliminates the overhead of constructing and updating routing tables. It consists of many phases; Firstly, the protocol will construct a logical tree between network nodes. During the construction each node will get a logical ID and construct its neighbors table. The messages flow of this phase is illustrated in Figure 4. When any *Ready* message is received, the receiver should store the information contained in the message in its neighbors table. Then the receiver will send an *Engagement* message to get an ID. If the engagement process completed successfully, then the receiver will broadcast its ID in a *Ready* message.

Secondly, the FEAR protocol will transmit data packets using neighbor links in a company with parent-child links. During this stage both intermediate nodes energy and depth will be considered. Finally, it will reconstruct the tree due to node(s)/link(s) failure (Figure 5) or new node entrance (Figure 6). As illustrated in Figure 5, the node will start the tree reconstruction when it receives an *Inform* message that contains the dead node ID. There are three cases; if the ID that is contained in the *Inform* message is a neighbor ID, then the node should remove this neighbor from its neighbors table.

Secondly, if the ID is a child ID, then the node should reduce its number of children. Finally, if it is a parent ID, then the node should find another parent by broadcasting *RequestParent* message. In Figure 6, the message flow for new node entrance is illustrated. Any new node should broadcast *NewNode* message. Other nodes will reply to this message by sending either *Ready* or *UnReady* message allowing the new node to be engaged to the network tree.

In both tree construction and reconstruction stages a fuzzy inference system will be used to rank the neighboring nodes according to specific factors. This rank is used to associate a particular node with the best possible parent among others in terms of remaining power, depth (number of hops to sink), and distance, thus keeps the balance between nodes.

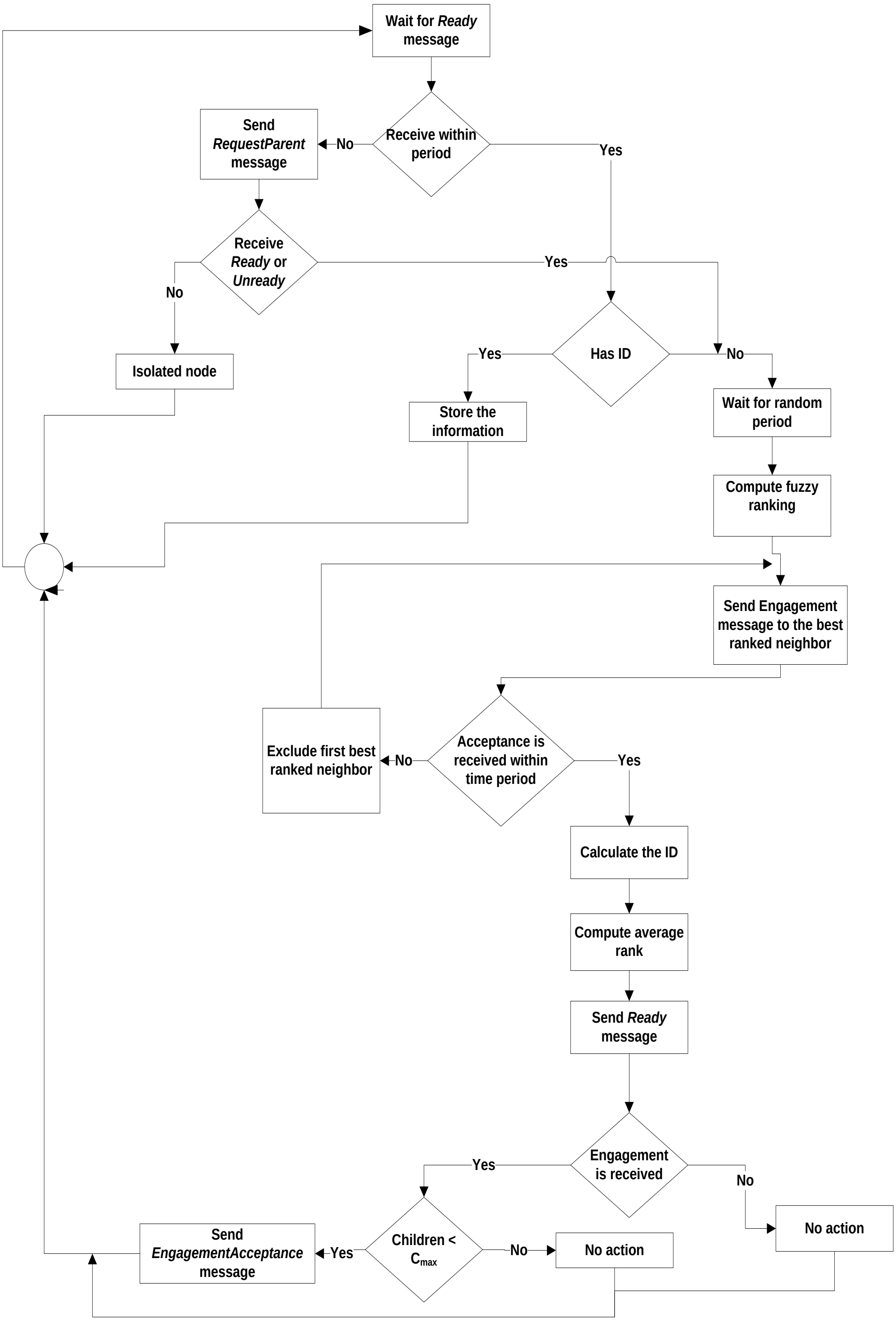


Figure 4: Messages flow during tree construction.

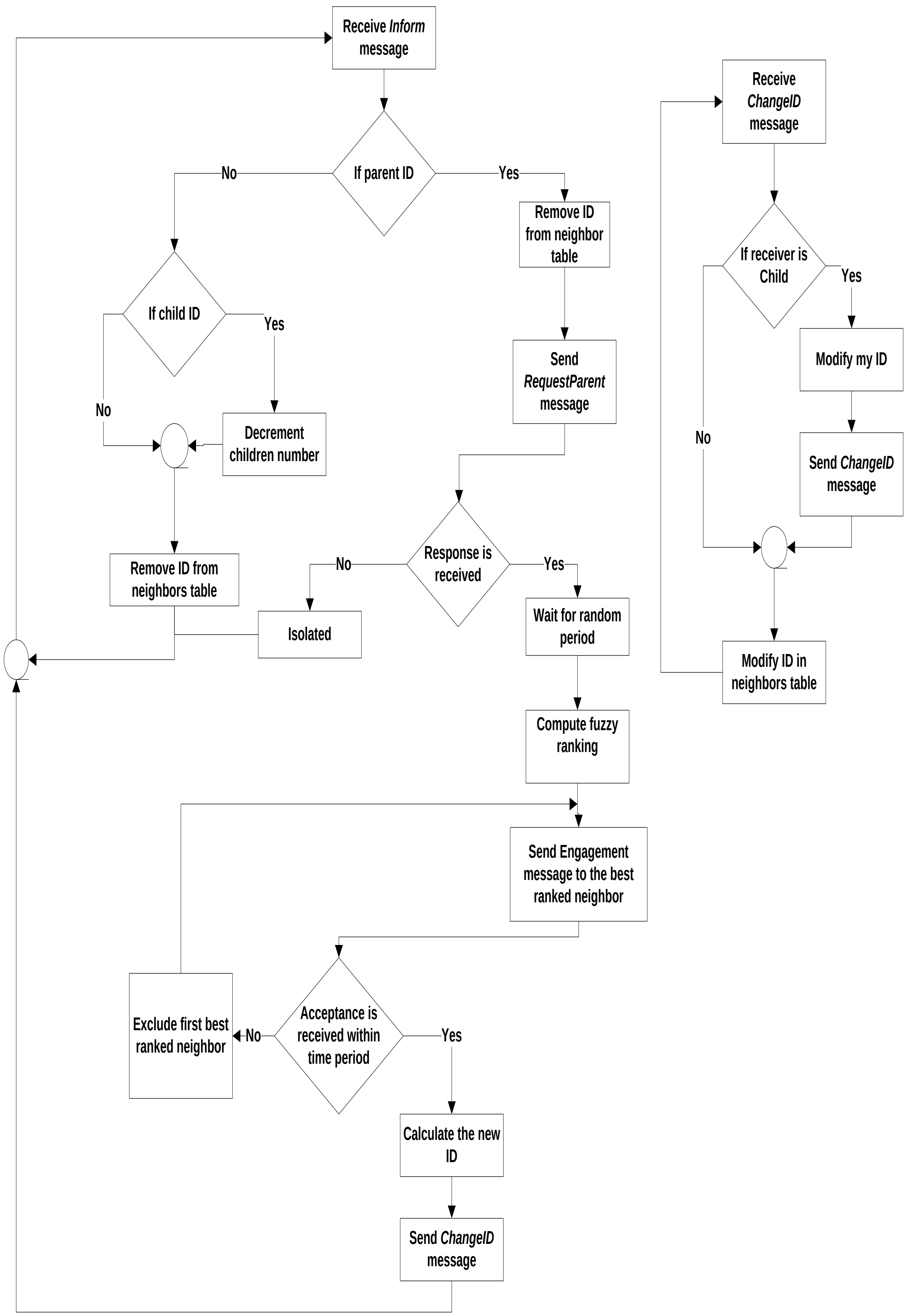


Figure 5: Messages flow during recovery from failure.

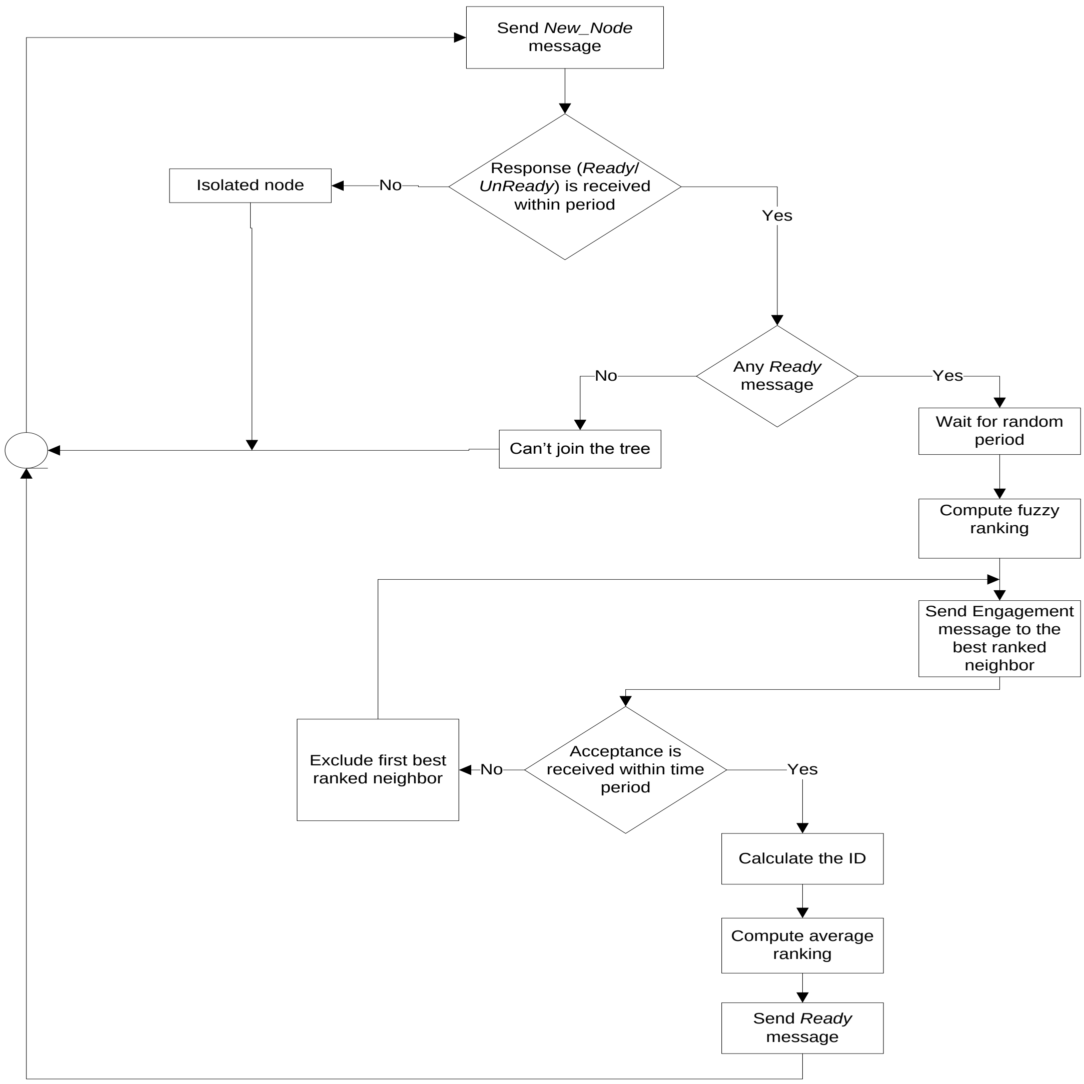


Figure 6: Messages flow during new node engagement.

Different control messages defined by FEAR protocol are needed to control the tree construction and reconstruction phases. These messages are: *Ready, Engagement, Engagement_Acceptance, UnReady, RequestParent, NewNode, Inform, and ChangeID*. Table 2 presents a brief description on these messages. The main disadvantages of FEAR protocol is that it does not consider security issues during its different phases. Attackers can easily bring the network down by overrunning its limited resources or distributing fake topological information between network nodes. The main idea in this thesis is to show that by applying an appropriate security schemes we can protect the

network from different security attacks. In the next subsection, the possible FEAR attacks and the impact of these attacks on the constructed topology will be discussed.

Table 2: FEAR control messages (ALmomani, et al., 2011).

Message	Purpose	Phase(s)
Ready	This message is sent by the node to broadcast its ID to its neighbors and tell other nodes that it is ready to accept children. It contains the sender ID, power, and status.	Tree Construction. Tree Reconstruction.
Engagement	This message is sent by the node to request an ID and request a parent.	Tree Construction. Tree Reconstruction.
Engagement_Acceptance	Is sent as a reply to an *Engagement* message. It contains sender ID, power, and the ID to be offered to the requesting node.	Tree Construction. Tree Reconstruction.
UnReady	This message is sent by the node to broadcast its ID to its neighbors.	Tree Reconstruction.
RequestParent	This message is sent when a node cannot reach its parent.	Tree Reconstruction.
NewNode	This message is sent when new node want to join the network.	Tree Reconstruction.
Inform	This message is sent by the node to tell the neighbors that the node will go down soon.	Tree Reconstruction.
ChangeID	This message is sent when any node change its ID due to any failure (e.g. the node change its parent). It tells other nodes to modify its ID in their neighbors' tables.	Tree Reconstruction.

3.2 FEAR Attacks

As discussed previously, FEAR protocol uses control messages to control the tree construction and reconstruction phases. Due to the absence of security defenses, attackers can utilize these messages to affect the topology construction and exchange wrong topological information between nodes. Table 3 illustrates the different types of FEAR attacks and their impact on the sensor network. As illustrated in the table,

different attacks can be performed on FEAR control messages; by sending large number of fake control messages the attacker can overrun nodes' resources, by eavesdropping on control messages' information the attacker can know network topology, and by modifying control messages' information the attacker can distribute wrong topological information between network nodes.

Table 3: FEAR attacks.

Control Message	Attack	Outcome
Ready	1- Send a large number of fake *Ready* messages.	1.1 Overrun neighbors' resources due to the cost of receiving, processing, and storing fake *Ready* messages. 1.2 Neighbors add the adversary node to their neighbors table.
	2- Eavesdrop on neighbors' *Ready* messages.	2.1 Adversary node knows network topology.
	3- Change the information contained in neighbors' *Ready* messages.	3.1 Neighbors store wrong topological information in their tables. 3.2 Affect the engagement process.
Engagement	1- Send a large number of fake *Engagement* messages.	1.1 Overrun neighbors' resources due to the cost of receiving, processing, and replying to fake *Engagement* messages. 1.2 Neighbors accept the adversary node as a child and send a reply (*Engagement_Acceptance*).
Engagement_Acceptance	1- Send a large number of fake *Engagement_Acceptance* messages.	1.1 Overrun neighbors' resources due to the cost of receiving and processing of fake *Engagement_Acceptance* messages. 1.2 Neighbors accept the adversary node as a parent.
	2- Change the information contained in neighbors' *Engagement_Acceptance* messages.	2.1 Neighbors get wrong Offered IDs; consequently, they will have wrong IDs. 2.2 Wrong topological information will be

		exchanged between nodes.
UnReady	1- Send a large number of fake *UnReady* messages.	1.1 Overrun neighbors' resources due to the cost of receiving, processing, and storing fake *UnReady* messages. 1.2 Neighbors add adversary node into neighbors table.
	2- Eavesdrop on neighbors' *UnReady* messages.	2.1 Adversary node knows network topology.
	3- Change the information contained in neighbors' *UnReady* messages.	3.1 Neighbors store wrong topological information in their tables.
RequestParent / NewNode	1- Send a large number of fake *RequestParent/ NewNode* messages.	1.1 Overrun neighbors' resources due to the cost of receiving, processing, and replying to fake *RequestParent/ NewNode* messages. 1.2 Neighbors may accept the adversary node as a child.
Inform	1- Send a large number of fake *Inform* messages.	1.1 Overrun neighbors' resources due to the cost of receiving, processing, and responding to fake *Inform* messages.
	2- Eavesdrop on neighbors' *Inform* messages.	2.1 Adversary node knows network topology.
	3- Change the information contained in neighbors' *Inform* messages.	3.1 Neighbors may exclude honest nodes from their neighbors table. Consequently, wrong topological information will be stored. 3.2 Wrong topology will be constructed between network nodes.
ChangeID	1- Send a large number of fake *ChangeID* messages.	1.1 Overrun neighbors' resources due to the cost of receiving, processing, and responding to fake *ChangeID* messages.
	2- Eavesdrop on neighbors' *ChangeID* messages.	2.1 Adversary node knows network topology.
	3- Change the information contained in neighbors' *ChangeID* messages.	3.1 Neighbors change neighbors' ID. Consequently, wrong topological

		information will be stored. 3.2 Wrong topological information will be exchanged between network nodes.

3.3 Securing the FEAR Protocol

In this subsection the security requirements and techniques that are needed to secure FEAR protocol will be discussed. In addition, we will describe how to apply these techniques on FEAR protocol.

As discussed in the previous section, many attacks can affect the constructed topology among network nodes by forcing network nodes to add adversary nodes to their tables and/or exchange wrong topological information between them. In both ways, the constructed topology is not secure to be used for data transmission. To protect the network among different external attacks some security prevention techniques must be applied to FEAR protocol. These techniques depend on the security requirements that need to be achieved. Our concern in this thesis is to establish a secure topology in order to be used in the data transmission phase to ensure correct and safe data forwarding. The secrecy of data itself is out of the scope of this thesis since it depends on the application of the WSN. For example military applications may require data to be encrypted while environment monitoring applications may not.

To establish a secure topology and exclude adversary nodes we need to make sure that all nodes that are participating in the construction phase are network sensors and not attackers. To achieve this, nodes authentication should be achieved. Another important requirement in order to ensure correct topological information is data

integrity. Attackers can modify important information in FEAR control messages allowing wrong topological information to be exchanged between nodes. For example, as we mentioned before, FEAR protocol uses fuzzy logic to rank sensor nodes according to specific parameters, modifying any parameter's value will affect the ranking process so we need to achieve data integrity between nodes.

3.3.1 Security Techniques

To achieve authentication and data integrity both Message Authentication Code (MAC) and Digital Signature (DS) schemes can be used. MAC algorithms are either hash based or block cipher based. In MAC algorithms the MAC value, which is also known as digest, is calculated according to a specific hash function or using block cipher techniques, then it is added to the message to be sent. To achieve authentication a shared key between the sender and the receiver is used in the digest calculation while integrity is achieved using an appropriate collision resistant hash function (Indesteege, 2010). On the other hand, DS uses Public Key Cryptography (PKC) to sign the message to be sent. This signature is calculated by encrypting the digest value using sender's private key. The verification process is done by decrypting the signature using sender's public key. In this way both integrity and authenticity are achieved. Although PKC techniques are not efficient to be used in WSNs due to its complexity and high processing and power requirements, Elliptic Curve Cryptography (ECC) is recently used in WSNs due to its low complexity comparing with other PKC techniques. In this thesis, Cipher Block Chaining- MAC (CBC- MAC) based on AES block cipher algorithm is used to calculate the MAC value due to its less power cost comparing with other cipher-based MAC algorithms (Lee, et al., 2010). Moreover, AES-128 is an efficient block cipher in terms of its security strength and its moderate key size. For DS,

Elliptic Curve Digital Signature Algorithm (ECDSA) which is based on ECC is used to sign the message.

Cipher Block Chaining MAC (CBC-MAC) is a technique for calculating MAC value based on a block cipher. The message is encrypted using the block cipher algorithm (AES in our case) in CBC mode to create a chain of blocks. The MAC value, which will be added to the message, is the value that is resulted from the encryption of the last block. It uses two different keys one key is used by the block cipher algorithms (CBC) and the other for the MAC calculation (Lee, et al., 2010) in this way any change to any plaintext bits will cause a significant change in the final encrypted block that cannot be predicted without knowing the block cipher key. Figure 7 illustrates the process of CBC-MAC using AES block cipher. The message will be divided into fixed size blocks (128 bits for AES CBC-MAC), then each block is encrypted using the AES algorithm. Note that for each block the XOR operation is performed with the output from the previous block.

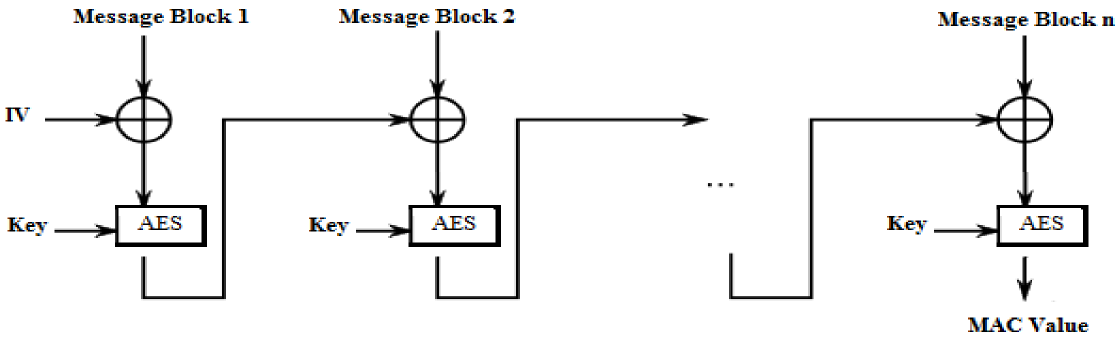


Figure 7: CBC-MAC processes (CBC11).

Elliptic Curve Digital Signature Algorithm (ECDSA) is a digital signature algorithm that is based on PKC to sign and verify messages. As other PKC based digital

signatures, ECDSA uses the private key in signature generation process. But before generating it, some public parameters should be exchanged between network nodes (Johnson, et al., 2001). These parameters are:

1- A field size q.

2- Two elements XG and YG to define a finite point $G = (XG, YG)$ of prime order.

3- The order n of the point G with $n > 2^{160}$ and $n > 4 * \text{sqrt}(q)$.

After parameter exchanging process any sender can generate a signature, which consists of two values; r and s, to sign the message to be sent. The signature generation process is done as the following assuming that d_A is sender's private key (Johnson, et al., 2001):

1. Calculate $e = H(m)$, where H is a hashing function and m is the message.
2. Select a random integer k from $[1, n - 1]$.
3. Calculate $r = x1 \pmod{n}$, where $x1 = k * G$. If $r = 0$, go to step 2.
4. Calculate $s = k - 1(e + d_A * r) \pmod{n}$. If $s = 0$, go to step 2.
5. The signature is the pair (r, s) that will be sent in the message.

When any node receives a signed message it can authenticate and verify its integrity using the sender's public key (Q_A) as the following (Johnson, et al., 2001):

1. Verify that r and s, which are received in the message, are integers in [1, n−1]. If not, the signature is invalid
2. Calculate $e = H(m)$, where H is a hashing function and m is the message.
3. Calculate $w = s - 1 \pmod{n}$.
4. Calculate $u1 = e * w \pmod{n}$ and $u2 = r * w \pmod{n}$.

5. Calculate $x1 = u1 * G + u2 * Q_A$.

6. The signature is valid if $x1 = r \pmod{n}$, invalid otherwise.

3.3.2 Applying Security Techniques to FEAR Protocol

This subsection will discuss how to apply CBC-MAC and ECDSA to secure the FEAR protocol. The use of authentication and data integrity techniques requires that all nodes agreed on shared key(s) or public keys before applying the security scheme. The following assumptions are considered:

1- All required keys are preloaded into network sensors.

2- All sensors are participating in the security verification process.

3- The sensors are scattered in the network field without isolation.

4- All sensor nodes have the same capabilities, the same transmission range, and limited power resource.

5- The symmetric model is assumed; which means if sensor A is within sensor B transmission range, then sensor B is within sensor A transmission range.

6- All sensors sense data and transmit it to the sink for processing.

7- The sink node is assumed to have unconstraint resources.

8- All sensor nodes are located in a fixed place without mobility.

During the different phases of FEAR protocol any control messages should be either signed or embedded with a MAC value. When any sensor receives a control message, it should verify whether this message is sent by an authenticated node or not. In addition, it should verify if it has been received without any modification otherwise the constructed topology will not be secure. Table 4 lists the main steps to achieve

secure network topology. It describes what should be performed before sending any control message and after receiving it.

Table 4: Steps to achieve security Requirements (Role of each node).

Sending Process	***Step 1.*** When any control message needs to be sent then apply CBC-MAC or ECDSA. ***Step 2.*** Add the calculated MAC value or the signature to the control message. ***Step 3***. Exit.
Receiving Process	***Step 1***. When any control message is received then apply CBC-MAC or ECDSA to verify the correctness of the message. ***Step 2.*** If the message is verified successfully then go to step 3 otherwise go to step 4. ***Step 3***. Process the message according to FEAR protocol procedures and go to step 5. ***Step 4.*** Ignore the message. ***Step 5.*** Exit.

Applying security schemes to achieve authentication and data integrity requires the sensor to perform local operations to verify the correctness of the message. This process will cost the sensor some of its power. In FEAR protocol, the main power consuming operations that all sensors perform are sending and receiving, thus most of the sensor power is consumed by communication operations. As stated by (Heinzelman, et al., 2000) the transmission and the receiving energy, $E_{Tx}(k,d)$ and $E_{Rx}(k)$ respectively, are calculated by Equations 1 and 2 respectively. According to Equation 1, the node requires $E_{Tx}(k,d)$ to send k bits message to destination at distance d, and according to Equation 2, the node requires $E_{Rx}(k)$ to receive k bits message.

$$E_{Tx}(k,d) = Eelec * k + Eamp * kd^2 \ldots (1)$$

$$E_{Rx}(k) = Eelec * k \ldots (2)$$

Where *Eelec* = 50 nJ/bit, and *Eamp* = 100 pJ/bit/m2. When applying security schemes, the local processing should be considered in the power consumption calculation. Therefore, sensor power will be consumed by both communication and processing operations. Equation 3 is used to measure the processing cost of one control message. This cost depends on two factors; number of message's blocks and the cost of processing one block.

$$\begin{gathered} Message\ Cost = NumOfBlocks\ \times BlockCost \\ where\ NumOfBlocks = \left\lceil \frac{MessageSize}{BlockSize} \right\rceil \end{gathered} \quad \ldots (3)$$

Where the BlockCost is the cost of processing one message block and it depends on the security mechanisms that is used. For CBC-MAC the cost of processing 128-bit block is 112.2 µJ when AES-128 block cipher is used where 128 is the key size in bits (Lee, et al., 2010). On the other hand, signing the message using ECDSA-160 will cost 6.26 mJ and verifying the signature cost is 12.41 mJ (Trakadas, et al., 2008). From Equation 3 we can calculate the processing cost of tree construction phase given the number of messages. According to the FEAR protocol the maximum number of messages that will be exchanged between nodes during tree construction phase is calculated by Equation 4. This number is proved in (ALmomani, et al., 2011).

$$\begin{gathered} SentMessages = 2N + \sum_{i=1}^{N} Ne(ni) \\ Received\ Messages = N + 2\sum_{i=1}^{N} Ne(ni) \end{gathered} \quad \ldots (4)$$

Where N is the number of nodes and $Ne(ni)$ is the number of neighbors for node i. For example assume that the size of a *Ready* message is 160 bits, then using CBC-MAC the message processing cost can be calculated as follows:

1. Number of blocks = 160/128 = 2
2. Message cost = 2 * 112.2 = 224.4 µJ

And using ECDSA the cost of signing and verifying the message is 6.26 + 12.41 = 18.67 mJ.

Chapter Four

Evaluation and Simulation Results

In this chapter the evaluation and simulation results will be discussed. QualNet 5.0 network simulator is used to simulate the protocol. Table 5 shows the hardware and software specifications that were used to perform the simulation in accompany with the simulation parameters that were used to conduct the scenarios. Different evaluation metrics are studied to evaluate the FEAR protocol with and without applying security schemes. These metrics will be discussed in the next subsections.

Table 5: Hardware and software specifications and simulation parameters.

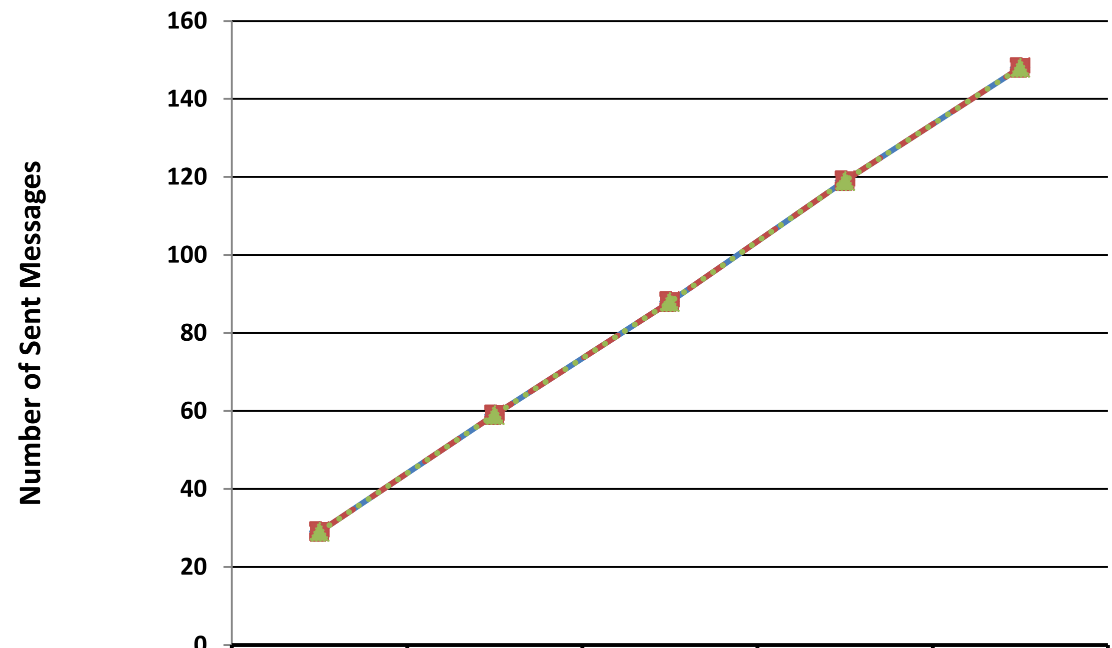
Hardware/Software	**Description**
CPU	Intel (R) core (TM) i3
RAM	4 GB
OS	Windows XP
Simulation Parameter	**Value**
Network Size	10, 20, 30, 40, and 50 nodes.
Terrain Area	1500 m X 1500 m
Mobility	None
Radio Range	250 m
Number of Sinks	1
Initial Energy	1000 J
Number of Attackers	10%, 20%, 30%, 40%, and 50 % from network size.

4.1 Security Cost

In this section we will evaluate the cost of applying CBC-MAC or ECDSA to secure the FEAR protocol. Both network overhead and power consumption are studied before and after applying the security mechanisms.

4.1.1 The Impact of Applying Security Schemes on the Network Overhead

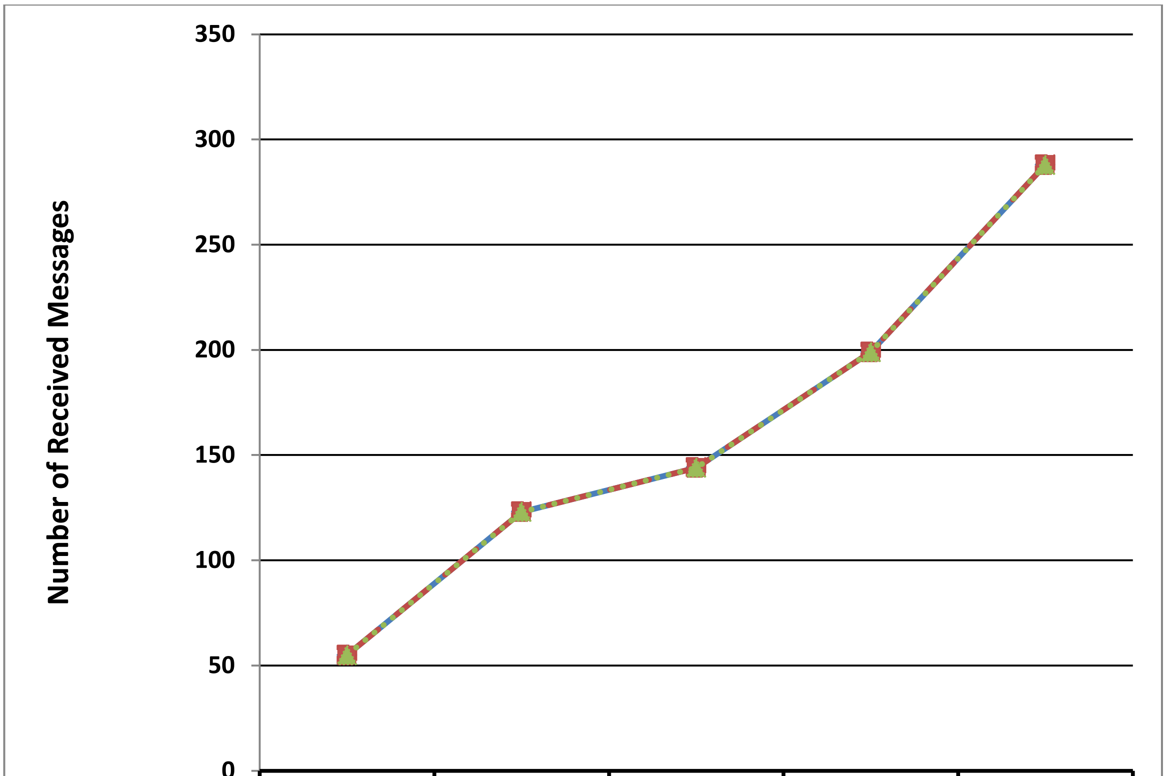
The overhead is evaluated in terms of number of messages that are sent and received between nodes. We use different network sizes 10, 20, 30, 40, and 50 nodes. For each size, the same nodes characteristics (initial power, nodes distribution, and distance from sink) are used for FEAR, FEAR-MAC, and FEAR-DS. Figures 8 and 9 show the number of sent and received messages of FEAR protocol before and after applying security mechanisms respectively. As illustrated in the figures, the overhead caused by the FEAR protocol does not change when applying CBC-MAC or ECDSA since it is applied on the same number of control messages that are needed to construct the tree without the need to exchange additional messages.



	10	20	30	40	50
FEAR	29	59	88	119	148
FEAR-MAC	29	59	88	119	148
FEAR-DS	29	59	88	119	148

Number of Nodes

Figure 8: Comparison between FEAR, FEAR-MAC, and FEAR-DS in terms of number of sent messages against different network sizes.



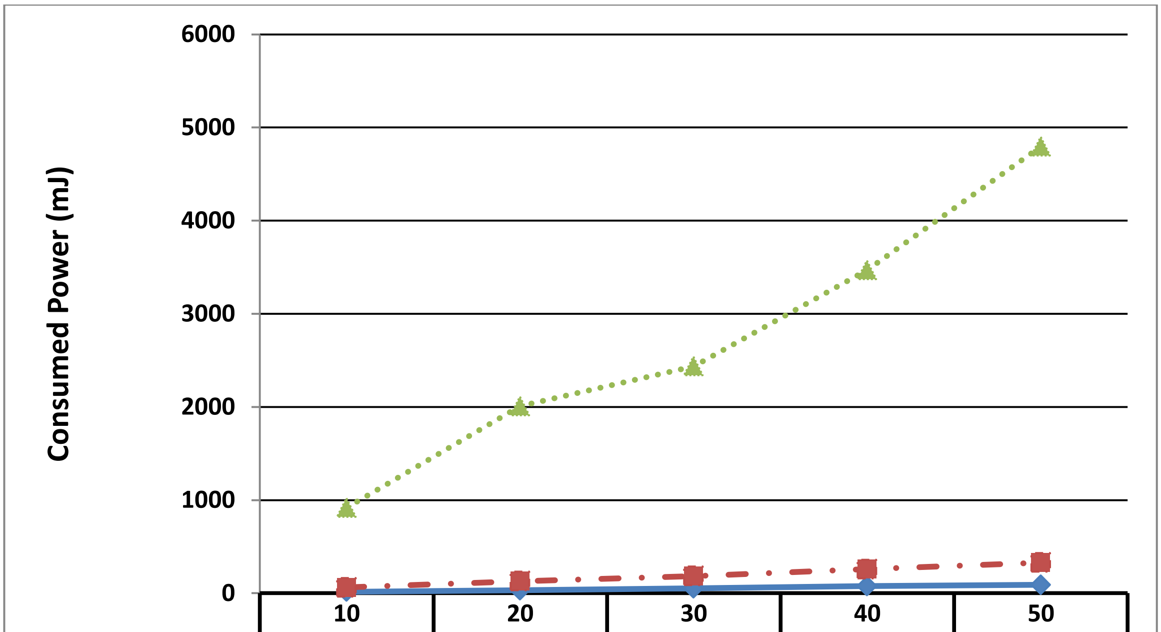
	10	20	30	40	50
FEAR	55	123	144	199	288
FEAR-MAC	55	123	144	199	288
FEAR-DS	55	123	144	199	288

Figure 9: Comparison between FEAR, FEAR-MAC, and FEAR-DS in terms of number of received messages against different network sizes.

4.1.2 The Impact of Applying Security Schemes on the Network Power Consumption

As we said previously, sensor power is consumed by communication and processing operations. Since all processing is done by the sink node, most of the sensor power is consumed by FEAR sending and receiving processes. When applying any security scheme the power that is consumed by local processing should be considered in a company with communication power. To obtain the power consumption results, we use the same simulation characteristics that are used in the overhead evaluation. The

results are shown in Figure 10. As illustrated in the figure, the consumed power increases when applying the security schemes and the results illustrate that using CBC-MAC will cost about 64 x 10^{-5} % from network power whereas ECDSA costs about 91 x 10^{-4} %. Note that asymmetric based security approach consumes more power than symmetric approach due to its complexity in signature generation and verification processes.



	10	20	30	40	50
FEAR	15	31	52	76	89
FEAR-MAC	63	130	184	258	329
FEAR-DS	919	2008	2436	3470	4795

Figure 10: Comparison between FEAR, FEAR-MAC, and FEAR-DS in terms of power consumption against different network sizes.

4.2 Effect of Routing Attacks

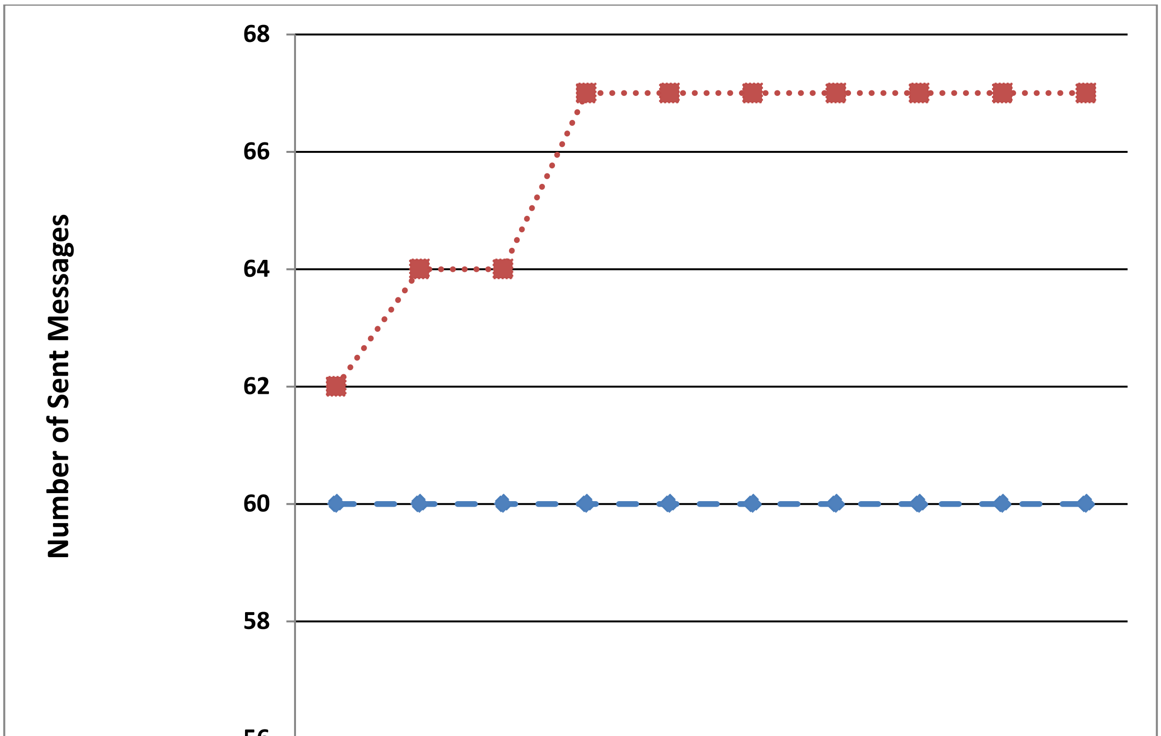
In this section we will evaluate the impact of external attackers on FEAR protocol in terms of network overhead and consumed power. Five different attacks are studied which are: *Ready* Attack, *Inform* attack, *ChangeID* attack, *RequestParent*

attack, and *NewNode* attack. Each attack is named according to the type of the fake control message that attackers send.

4.2.1 Effect of Attacks on the Network Overhead

Also, in this section the overhead is evaluated in terms of number of sent and received messages. Each attack starts after 3000 second from the beginning of the simulation time by sending one fake control message per second until the simulation stops after 20000 seconds. The results of the number of sent messages are shown in Figures 11 and 12 (the results are split into two figures due to the scaling gap). In Figure 11 the results of *Ready* and *Inform* attacks are illustrated. For *Ready* attack, the number of sent messages remain constant (60 messages) after 2000 seconds from the beginning of the simulation time. This is because *Ready* attacks are performed by sending fake *Ready* messages. The receiving of *Ready* message (by network sensors) does not require the receiver to send any control message as a reply to that *Ready* message. On the other hand, *Inform* attacks affect the number of sent messages during the time interval from 2000 to 8000 seconds. The reason is that some attackers are parents to some sensor nodes. Parent attacker sends fake *Inform* massage tilling its children that it will go down, thus the children should find another parent through the tree reconstruction phase (see Figure 5). This reconstruction requires extra messages to be exchanged between network nodes.

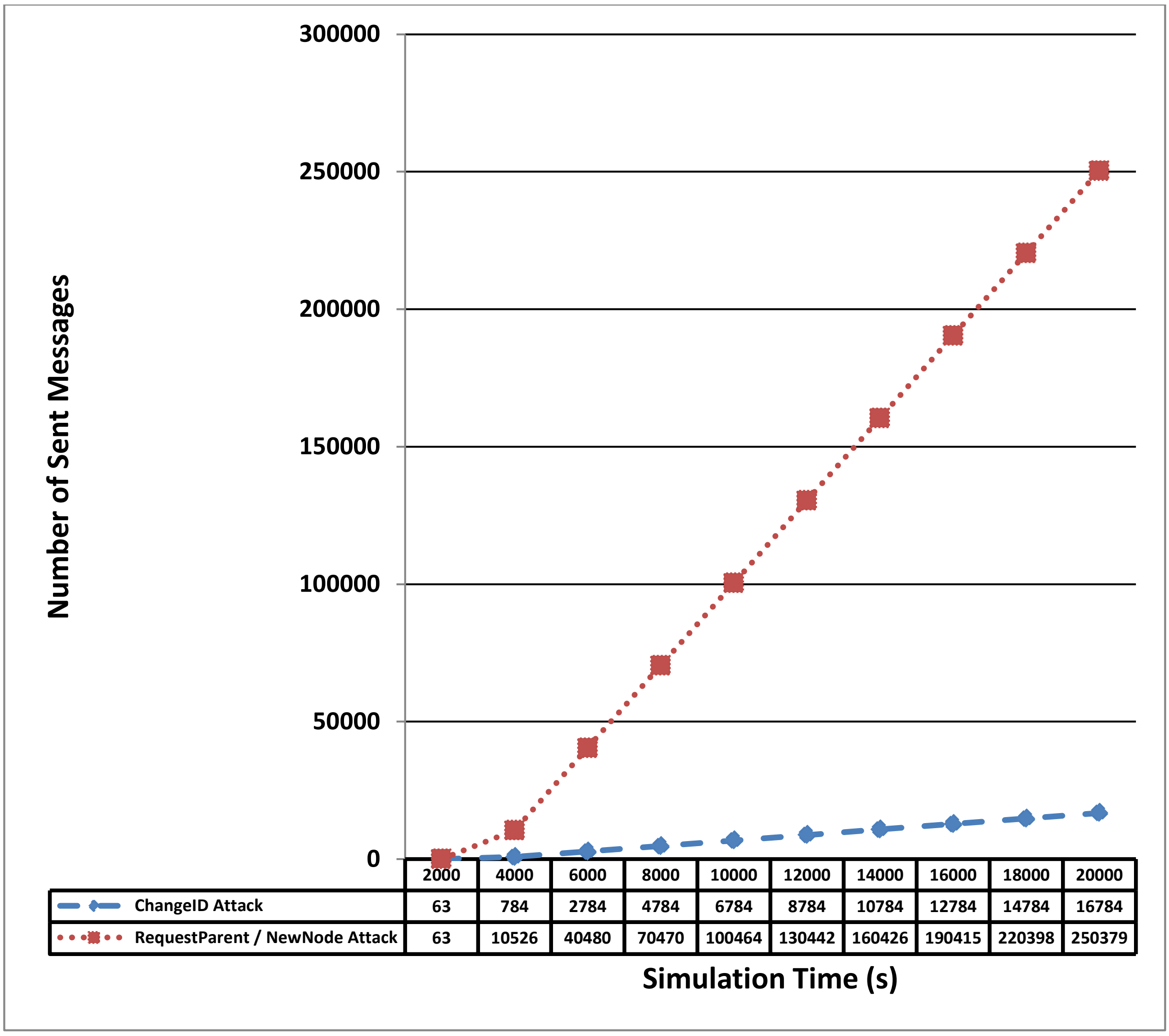
After 8000 seconds, the reconstruction phase is completed and all parent attackers are excluded. Consequently, the number of sent messages remains constant until the end of the simulation. Note that the *Inform* attacks remain active until the end of the simulation, but after 8000 seconds it will only affect the number of received messages.



	2000	4000	6000	8000	10000	12000	14000	16000	18000	20000
Ready Attack	60	60	60	60	60	60	60	60	60	60
Inform Attack	62	64	64	67	67	67	67	67	67	67

Figure 11: The effect of Ready and Inform attacks on number of sent messages against simulation time.

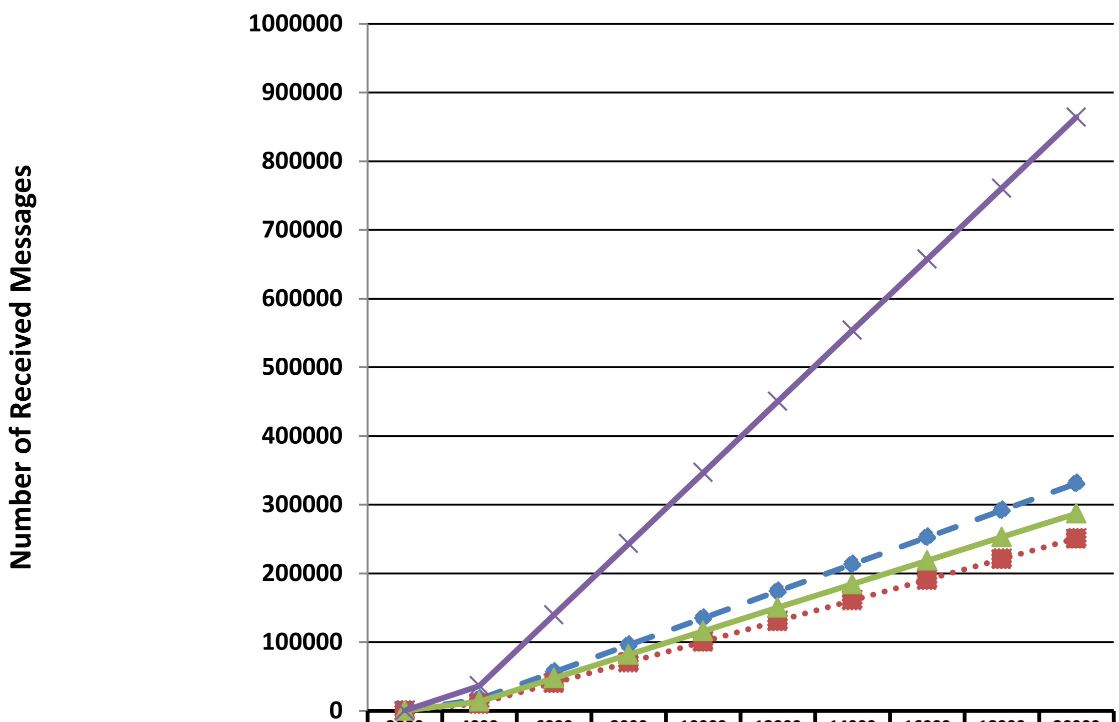
In Figure 12, the results of *ChangID*, *RequestParent*, and *NewNode* attacks are illustrated. Unlike other attacks *RequestParent* and *NewNode* attacks significantly increase the number of sent messages since all neighbors (attackers' neighbors) will reply to these attacks by sending *Ready* or *UnReady* messages (see Figures 4 and 6). On the other hand, *ChangeID* attack affects only children nodes. When any child (attacker's child) receives fake *ChangeID* message it will send *ChangeID* message (see Figure 5). Thus only children are affected by this attack in term of number of sent messages.



	2000	4000	6000	8000	10000	12000	14000	16000	18000	20000
ChangeID Attack	63	784	2784	4784	6784	8784	10784	12784	14784	16784
RequestParent / NewNode Attack	63	10526	40480	70470	100464	130442	160426	190415	220398	250379

Figure 12: The effect of ChangeID, RequestParent, and NewNode attacks on the number of sent message aganst simulation time.

The results of the number of received messages are shown in Figure 13. As illustrated in the figure, *RequestParent* and *NewNode* attacks increase the number of received messages in a significant way since neighbor nodes will reply to these attacks by sending either *Ready* or *UnReady* messages in a broadcast manner affecting all nodes in their ranges.



	2000	4000	6000	8000	10000	12000	14000	16000	18000	20000
Ready Attack	115	17029	56294	95600	134843	173993	213230	252477	291741	330978
Inform Attack	123	10447	40495	70548	100646	130707	160703	190805	220861	250983
ChangeID Attack	125	13352	47540	81762	116015	150209	184387	218626	252874	287110
RequestParent / NewNode Attack	126	36191	139545	243169	346806	450460	553895	657300	760545	863980

Simulation Time (s)

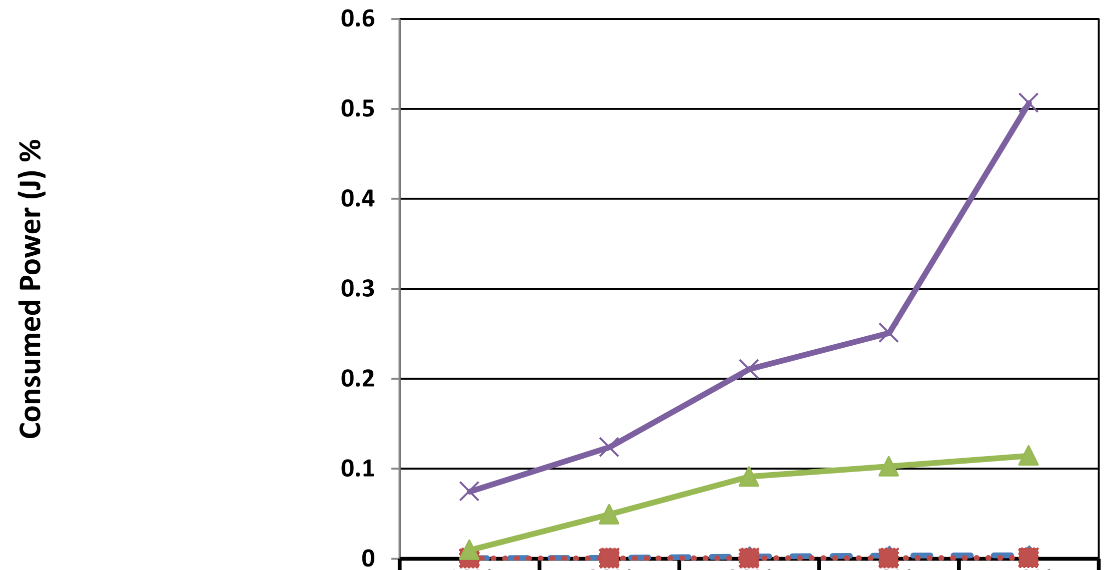
Figure 13: The effect of different FEAR attacks on the number of received message against simulation time.

4.2.2 Effect of Attacks on Network Power Consumption

Since no local processes and verifications are required in FEAR protocol, the consumed power depends on the number of sent and received messages which can be calculated using Equations 1 and 2. The results are obtained according to two different scenarios. Firstly, we find the impact on network power according to different percentage of attacker; 10%, 20%, 30%, 40%, and 50% of network size. The simulation time is 6000 seconds. The results are shown in Figure 14. As illustrated in the figure, the larger the number of attackers the more the power is consumed. Moreover,

RequestParent, *NewNode*, and *ChangeID* attacks consume more power than other attacks due to the large overhead caused by these attacks.

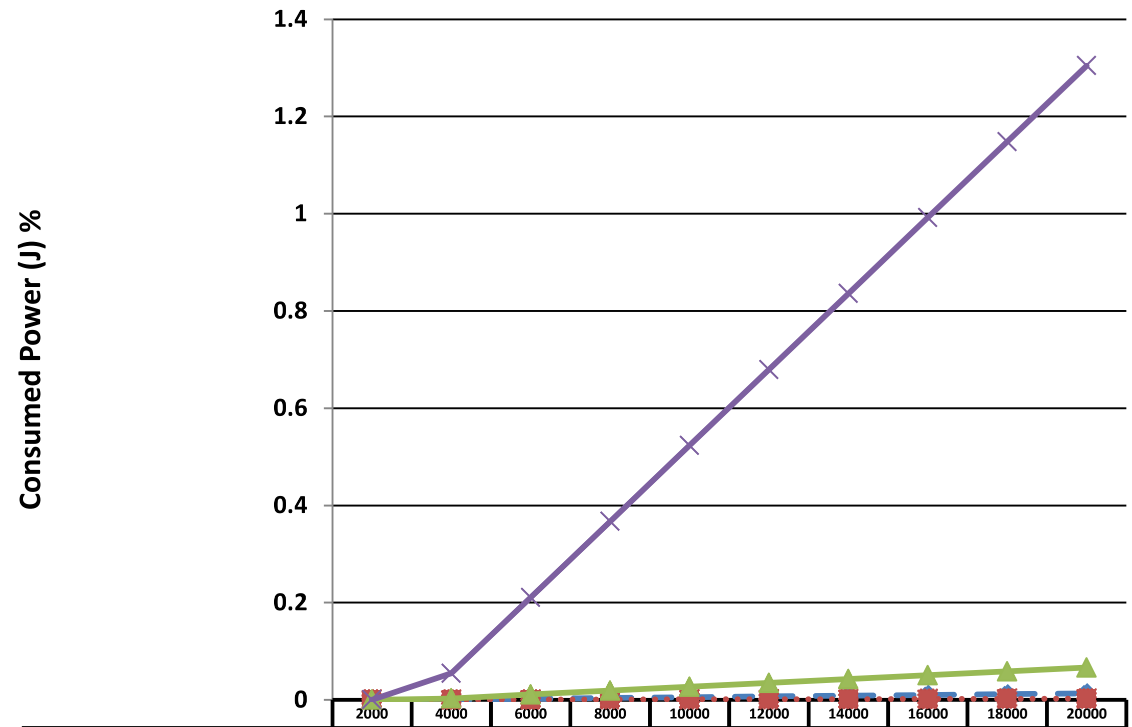
Secondly, we find the impact of attackers on network power against simulation time. The results are illustrated in Figure 15. The number of attackers is fixed for all attacks which is 30% of network size. As illustrated in the figure, increasing attacks duration will increase the consumed power since the overhead increases too. According to the conducted scenarios the attacks could consume up to 1.3 % from network power after 20000 seconds.



	10%	20%	30%	40%	50%
Ready Attack	0.000785	0.001045	0.00242	0.00331	0.003735
Inform Attack	0.000305	0.00036	0.000545	0.000625	0.00089
ChangeID Attack	0.009585	0.04919	0.091115	0.102535	0.11443
RequestParent/NewNode Attack	0.0746	0.123845	0.21067	0.25097	0.50646

Attackers Percentage

Figure 14: The effect of different FEAR attacks on network power.



	2000	4000	6000	8000	10000	12000	14000	16000	18000	20000
Ready Attack	0.000165	0.000845	0.00242	0.00399	0.00556	0.007125	0.008695	0.010265	0.01184	0.0134
Inform Attack	0.000185	0.00027	0.000545	0.000835	0.00112	0.001395	0.001675	0.00195	0.00223	0.002505
ChangeID Attack	0.00019	0.00307	0.01099	0.018925	0.02686	0.03478	0.04272	0.050645	0.058585	0.06651
RequestParent/NewNode Attack	0.00018	0.054595	0.21067	0.36696	0.523255	0.67947	0.83571	0.99197	1.148195	1.30442

Figure 15: Effect of different FEAR attacks on network power against simulation time.

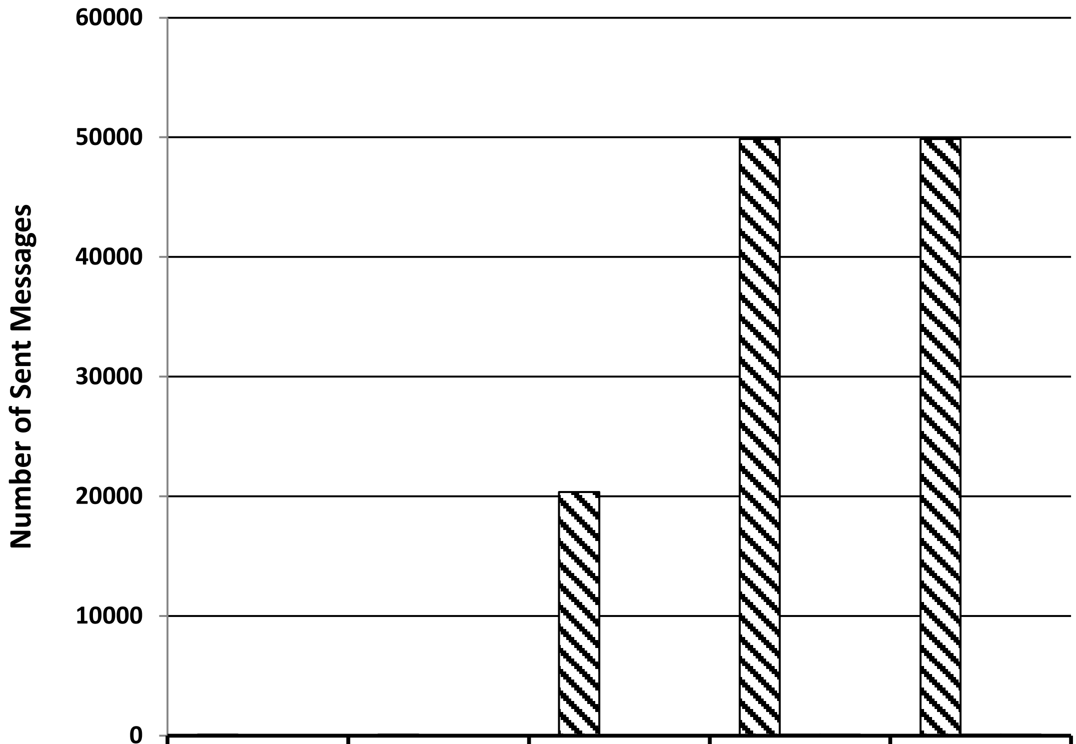
4.3 The Impact of Attackers on Secure FEAR

In this section we will study the impact of attackers when applying CBC-MAC or ECDSA on FEAR protocol and compare them with unsecure FEAR protocol. Three evaluation metrics are studied; network overhead, network consumed power, and network topology. The following subsections will discuss the results.

4.3.1 Network Overhead and Power Consumption

We compare the overhead and the power consumption that are caused by external attacks before and after applying security mechanisms. The same scenario characteristics are used to evaluate the three approaches (FEAR, FEAR-MAC, and

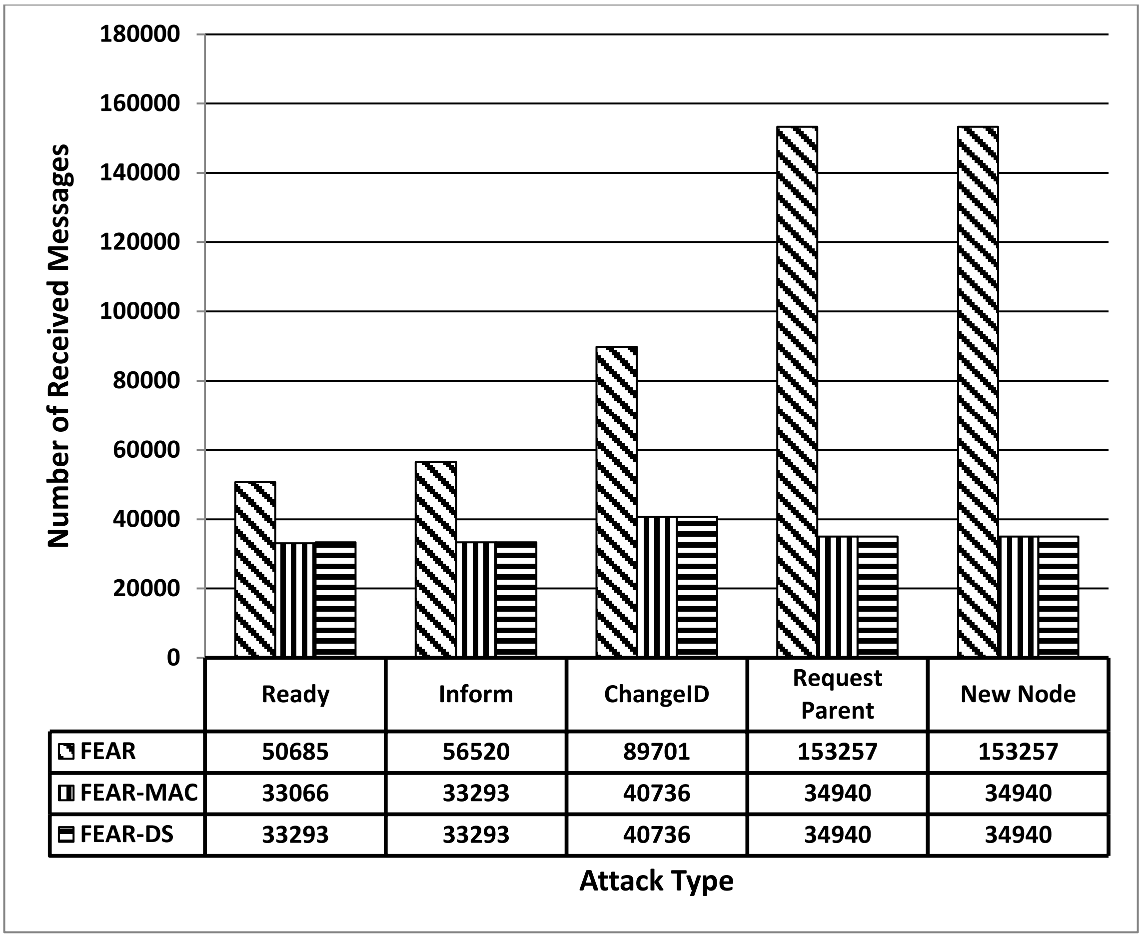
FEAR-DS). The results of sent and received messages are shown in Figures 16 and 17, respectively, where the results of power consumption are shown in Figure 18. According to network overhead, applying security mechanisms (either CBC-MC or ECDSA) will decrease the effect of attackers since sensors will not respond to adversary nodes, consequently the number of exchanged messages will be reduced. Note that *Ready* and *Inform* attacks do not affect the number of sent messages (as discussed in section 4.2.1).



	Ready	Inform	ChangeID	Request Parent	New Node
FEAR	59	69	20345	49858	49858
FEAR-MAC	57	57	56	58	58
FEAR-DS	57	57	56	58	58

Attack Type

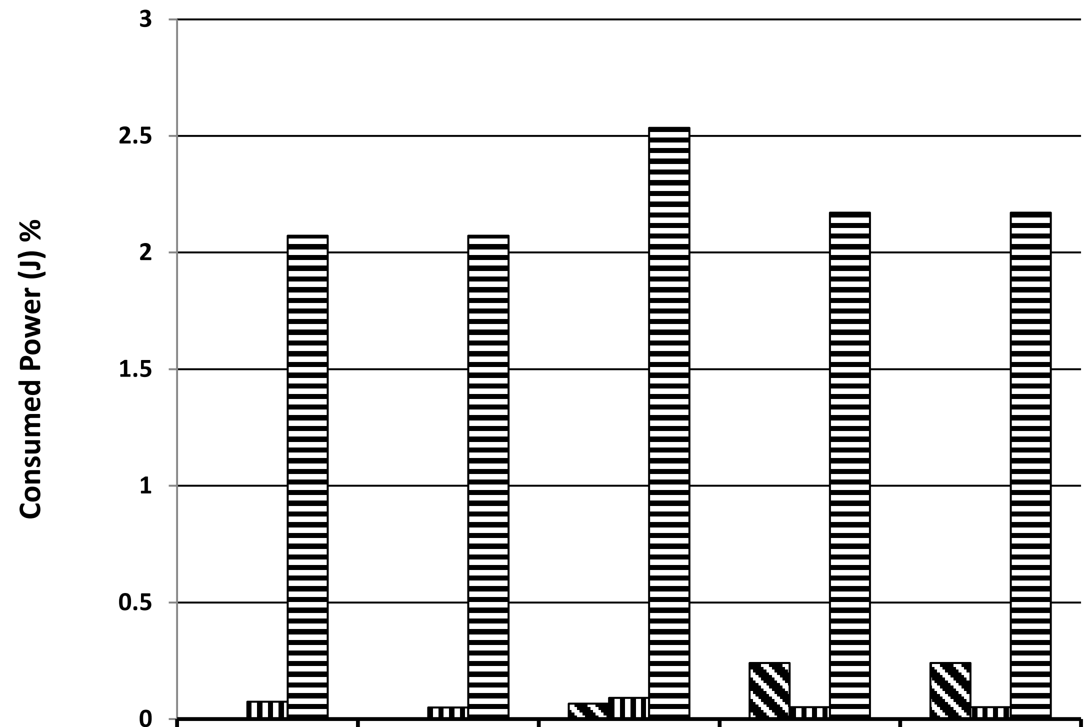
Figure 16: A comparison between FEAR, FEAR-MAC, and FEAR-DS in terms of the effect of different FEAR attacks on the number of sent messages.



	Ready	Inform	ChangeID	Request Parent	New Node
FEAR	50685	56520	89701	153257	153257
FEAR-MAC	33066	33293	40736	34940	34940
FEAR-DS	33293	33293	40736	34940	34940

Figure 17: A comparison between FEAR, FEAR-MAC, and FEAR-DS in terms of the effect of different FEAR attacks on the number of sent messages.

According to the consumed power (Figure 18) the results show that some attacks (*RequestParent* and *NewNode*) will cost the network about 4.7 times the cost that is required when security requirements are applied using CBC-MAC technique. This value is calculated by dividing 0.241125, which is the cost of FEAR protocol under *RequestParent* and *NewNode* attacks, over 0.0513, which is the cost of FEAR protocol under the same attacks using CBC-MAC. On the other hand, other attacks cost the network more when security schemes are applied due to the verification process of fake messages. Moreover, as illustrated in the figure, the DS scheme is the most power consuming due to its complexity comparing with MAC scheme.



	Ready	Inform	ChangeID	Request Parent	New Node
FEAR	0.002215	0.000645	0.06584	0.241125	0.241125
FEAR-MAC	0.075035	0.05042	0.091705	0.0513	0.0513
FEAR-DS	2.072505	2.071435	2.534595	2.17078	2.17078

Attack Type

Figure 18: A comparison between FEAR, FEAR-MAC, and FEAR-DS in terms of the effect of different FEAR attacks on the power consumption.

4.3.2 Network Topology

In this subsection the impact of attackers on network topology is assessed before and after applying security schemes. Two scenarios are used with different number of attackers (20% and 50% respectively). In Figure 19, the network consists of 10 normal nodes and 2 attackers which are nodes 21 and 22. When applying the FEAR protocol (Figure 19(b)) all attackers will participate in the tree construction phase and will be treated as normal nodes. In this scenario, the tree construction is started by node 1 which gets logical ID 0 and broadcast a *Ready* message to other nodes. Attacker 21

engaged to node 0 with ID 03. Same for attacker 22 that engaged to node 02 with ID 021. The tree construction is continued until all nodes, including attackers, got an ID. Thus, in FEAR protocol, attackers can join the constructed tree which will lead to unsecure topology construction.

On the other hand, applying CBC-MAC or ECDSA excludes all attackers from the constructed tree since they are not authenticated (Figure 19(c)). Consequently, the topology is kept secure and can be used to transmit data packets safely and securely between network nodes.

Same process is applied on scenario 2 with 5 attackers (Figure 20(a)) which are nodes 21 - 25. As in the first scenario, applying the FEAR protocol without applying security techniques will result in unsecure topology, since attackers join the constructed tree (Figure 20(b)). But when applying CBC-MAC or ECDSA all attackers will be excluded from the tree (Figure 20(c)).

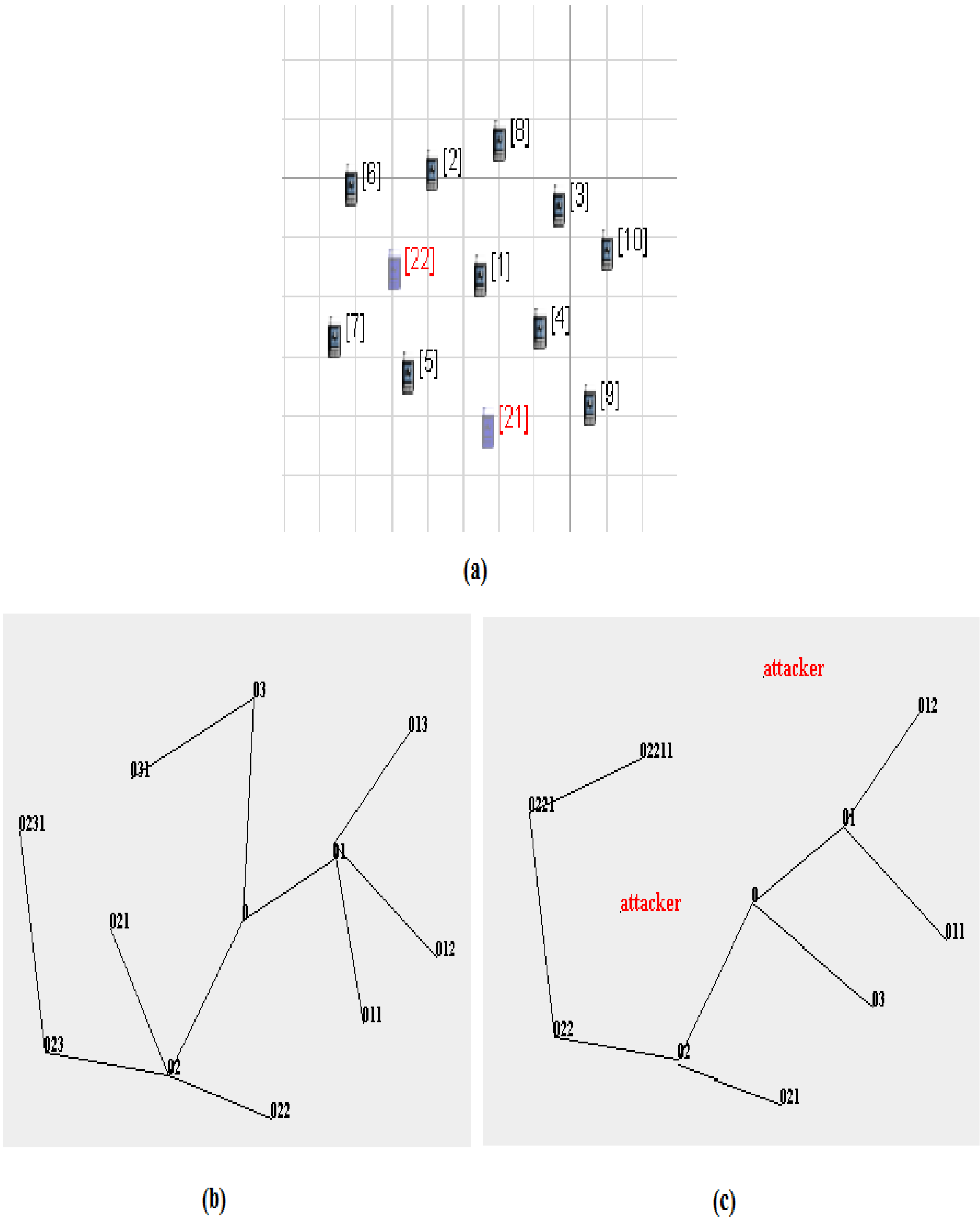


Figure 19: The effect of attackers on network topology, (a): The network field wilth 20 % attackers, (b): The constructed tree before applying security schemes, (c): The constructed topology after aplying security schemes.

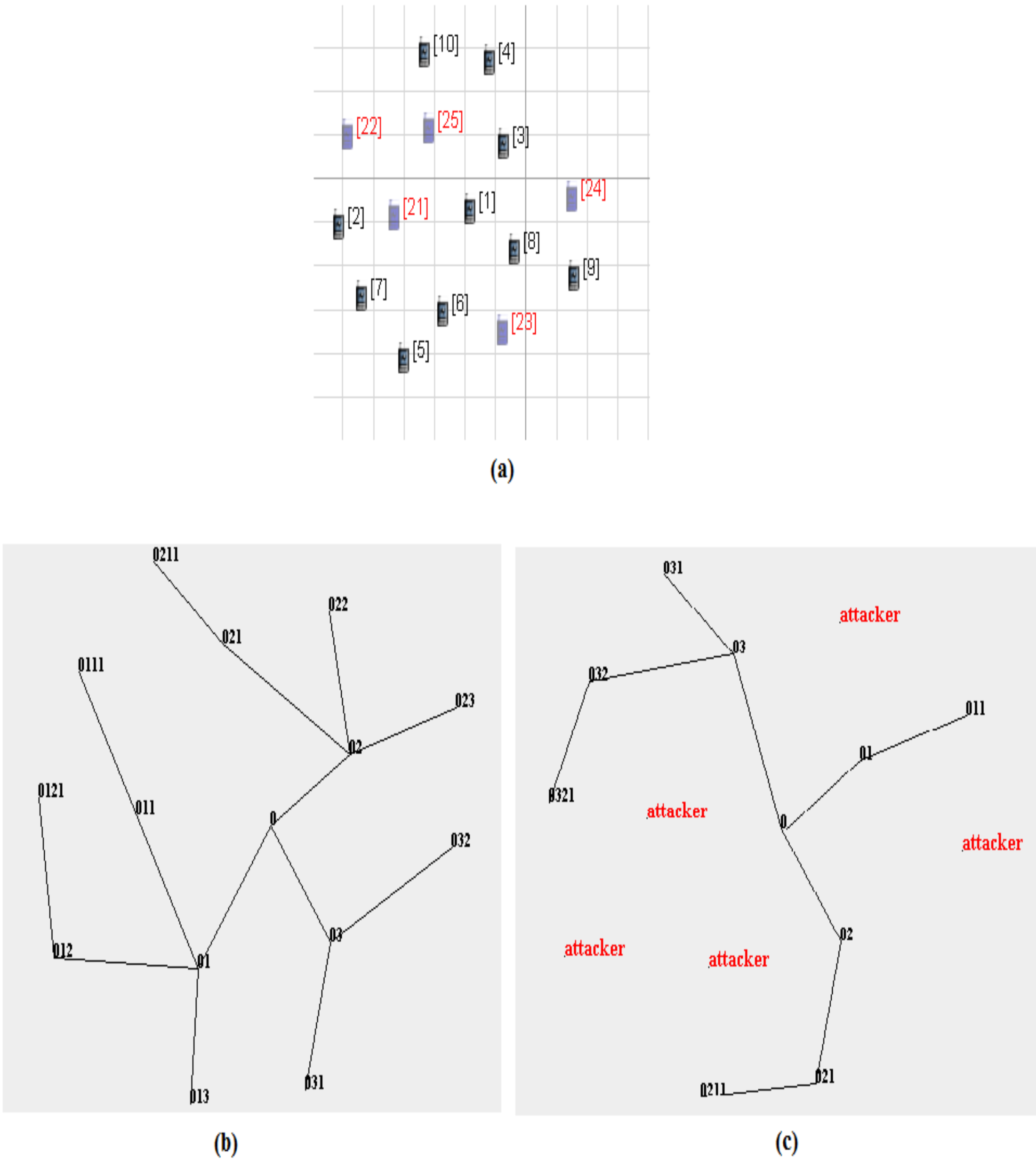


Figure 20: The effect of attackers on network topology, (a): The network field wilth 50 % attackers, (b): The constructed tree before applying security schemes, (c): The constructed topology after aplying security schemes.

Chapter Five
Conclusions and Future Work

5.1 Conclusions

In this thesis the FEAR protocol is improved by applying some security mechanisms to build an energy efficient secure routing protocol that protects the network against different external attacks. The main goal is to build a secure topology among network nodes to be used for secure data transmission. To achieve this, both authentication and data integrity should be achieved. We apply CBC-MAC and ECDSA security schemes to achieve the needed security requirements based on symmetric and asymmetric approaches, respectively.

QualNet simulator is used to assess the impact of attackers on network topology and routing process in FEAR, FEAR-MAC, and FEAR-DS protocols. In addition, we have compared the cost of securing the FEAR protocol using different security schemes based on symmetric and asymmetric security approaches. After applying security schemes, the results show that CBC-MAC will cost 0.00064 % of network power and ECDSA costs about 0.0091 %. Although this cost is required to achieve the needed security requirements, the results also show that some attackers will cost the network about 4.7 times the cost of achieving these requirements.

Moreover the results reveal that considering only the resource limitations of sensor nodes is not enough to develop an efficient routing protocol without protecting the network from different routing attacks since attackers can drop network power by time. Regarding network topology achieving authentication and data integrity excludes all attackers from network topology. Consequently, the constructed topology can be used for secure data transmission.

5.2 Future Work

As a future work we will conduct a study to evaluate other security schemes that could cost less power to assess their efficiency in achieving the needed security requirement. In addition to that, the internal attacks will be considered by applying a well defined Intrusion Detection System (IDS) to detect and exclude compromised nodes from the network.

References

Abuhelaleh, M., Mismar, T., & Abuzneid, A. (2008). Armor-LEACH – Energy Efficient, Secure Wireless Networks Communication, **Proceedings of 17th International Conference on Computer Communications and Networks, ICCCN '08,** pp.1-7, US Virgin Islands.

Akkaya, K., & Younis, M. (2005). A Survey on Routing Protocols for Wireless Sensor Networks, **Ad Hoc Networks,** Vol.3, No.3, pp.325–349.

Akyildiz, I., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: a survey, **Computer Networks,** Vol.38, No.4 , pp.393–422.

Al-Harbawi, M., Rasid, M., & Noordin, N. (2009). Improved Tree Routing (ImpTR) Protocol for ZigBee Network, **International Journal of Computer Science and Network Security,** Vol.9, No.10, pp.146 - 152.

Al-Karaki, J., & Kamal, A. (2004). Routing Techniques in Wireless Sensor Networks: A Survey, **IEEE Wireless Communications,** Vol.11, No.6, pp.6-28.

Almazaydeh, L., Abdelfattah, E., Al- Bzoor, M., & Al- Rahayfeh, A. (2010). Performance Evaluation of Routing Protocols in Wireless Sensor Networks, **International Journal of Computer Science and Information Technology,** Vol.2, No.2, pp.64-73.

ALMomani, I., & Saadeh, M. (2011). FEAR: Fuzzy-Based Energy Aware Routing Protocol for Wireless Sensor Networks, **Int'l J. of Communications, Network and System Sciences,** Vol.4, No.6, pp.403-415.

Biradar, R., Patil, V., Sawant, S., & Mudholkar, R. (2009). Classification and Comparison of Routing Protocols in Wireless Sensor Networks, **Special Issue on Ubiquitous Computing Security Systems, UbiCC Journal,** Vol.4, pp.704-711.

CBC-MAC, accessed on 7 12, 2011, URL address **http: //pediaview.com/ openpedia/ CBC-MAC.**

Dimitriou, T., & Ioannis, K. (2008). Security Issues in Biomedical Wireless Sensor Networks, **First International Symposium on Applied Sciences on Biomedical and Communication Technologies, ISABEL,** pp.1 – 5, Aalborg, Danmark.

Gupta, S., Verma, H., & Sangal, A. (2010). Authentication Protocol for Wireless Sensor Networks, **World Academy of Science, Engineering and Technology, WASET,** Vol.66, pp.643 – 649, Paris, France.

Heinzelman, W., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-Efficient Communication Protocol for Wireless Microsensor Networks, **Proceedings of the 33rd Hawaii International Conference on System Sciences,** Vol.8, pp.3005-3014, Hawaii, USA.

Heinzelman, W., Sinha, A., Wang, A., & Chandrakasan, A. (2000). Energy-Scalable Algorithms And Protocols For Wireless Microsensor Networks, **Proceeding on IEEE International Conference on Acoustics, Speech, and Signal Processing , ICASSP,** Vol.6. pp.3722-3725, Istanbul, Turkey.

IEEE. (2005). **ZigBee Specification Version 1.0, ZigBee Alliance**, IEEE.

Indesteege, S. (2010). **Analysis and Design of Cryptographic Hash Functions**, Belgium: Katholieke Universiteit Leuven.

Intanagonwiwat, C., Govindan, R., & Estrin, D. (2000). Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks, **Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom_00,** pp. 56-67, Boston, UAS.

Jamalipour, A., & Zheng, J. (2009). Wireless Sensor Networks: A Networking Perspectiv,. Copyright © 2009 **Institute of Electrical and Electronics Engineers.**

Johnson, D., Menezes, A., & Vanstone, S. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). **International Journal of Information Security,** Vol.1, No.1, pp.36-63.

Jung, E.-S., & Yongsuk, P. (2007). Plus-Tree: A Routing Protocol For Wireless Sensor Networks, **Lecture Notes in Computer Science, LNCS,** Vol.4413, editors: Marcin S.

Szczuka, Daniel Howard, Dominik Sle¸zak, Haeng-kon Kim, Tai-hoon Kim, Il-seok Ko, Geuk Lee and Peter M.A. Sloot, pp.638 – 646.

Kanjee, M., Divi, K., & Liu, H. (2010). A Physiological Authentication Scheme in Secure Healthcare Sensor Networks, **7th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks ,SECON,** pp. 1 – 3, Boston, USA.

Kulik, J., Heinzelman, W., & Balakrishnan, H. (2002). Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks, **Wireless Networks,** Vol.8, No.2-3, pp.169–185.

Lee, J., Kapitanova, K., & Son, S. (2010). The price of security in wireless sensor networks. **Computer Networks,** Vol.54, No.17, pp.2967–2978.

McGrath, M., & Dishongh, T. (2010). **Wireless Sensor Networks for Healthcare Applications, Artech House.**

Mohajerzadeh, A., & Yaghmaee, M. (2010). Tree Based Energy and Congestion Aware Routing Protocol for Wireless Sensor Networks. **Wireless Sensor Network,** Vol.2, No.2, pp.161-167.

Mukesh, R., Damodaram, A., & Bharathi, S. (2009). Energy Efficient Security Architecture for Wireless Bio-Medical Sensor Networks, **International Journal of Computer Science and Information Security, IJCSIS,** Vol.6, No.1, pp.116-122.

Neves, P., Stachyra, M., & Rodrigues, J. (2008). **Application of Wireless Sensor Networks to Healthcare Promotion.**

Papadimitriou, A., Le Fessant, F., Viana, A., & Sengul, C. (2009). Cryptographic Protocols to Fight Sinkhole Attacks on Tree-based Routing in Wireless Sensor Networks, **5th Workshop on Secure Network Protocols ,NPSec,** pp.43 – 48, Princeton.

Pathan, A.-S. K., & Hong, C. S. (2007). A Secure Energy-Efficient Routing Protocol for WSN, **Parallel and Distributed Processing and Applications ,Lecture Notes in Computer Science,LNCS,** Vol.4742, pp.407–418.

Perkins, C., & Royer, E. (1999). Ad hoc on-demand distance vector routing, **Proceedings of Second IEEE Workshop Mobile Computing Systems and Applications,** pp. 90-100, New Orleans, USA.

Qiu, W., Skafidas, E., & Hao, P. (2009). Enhanced Tree Routing for Wireless Sensor Networks, **Ad Hoc Networks,** Vol.7, No.3, pp.638 – 650.

Ren, K., Lou, W., Zeng, K., & Moran, P. (2007). On Broadcast Authentication in Wireless Sensor Networks. **IEEE Transactions on Wireless Communications**, Vol.6, No.11, pp.4136 - 4144.

Söderlund, R. (2006). **Energy Efficient Authentication in Wireless Sensor Network**, Linköpings university.

Stavroua, E., & Pitsillidesa, A. (2010). A Survey on Secure Multipath Routing Protocols in WSNs, **Computer Networks,** Vol.54, No.13, pp.2215 – 2238.

Trakadas, P., Zahariadis, T., Leligou, H., Voliotis, S., & Papadopoulos, K. (2008). Analyzing Energy and Time Overhead of Security Mechanisms in Wireless Sensor Networks, **15th International Conference on Systems, Signals and Image Processing, IWSSIP**, pp. 137 – 140, Bratislava.

Villalba, L., Orozco, A., Cabrera, A., & Abbas, C. (2009). Routing Protocols in Wireless Sensor Networks, **Sensors,** Vol.9, No.11, pp.8399 -8 421.

Xu, Y., Heidemann, J., & Deborah, E. (2001). Geography informed Energy Conservation for Ad Hoc Routing, **Proceedings of the 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking, MobiCom_01,** pp.70 – 84, Rome, Italy.

Yeh, H.-L., Chen, T.-H., Liu, P.-C., Kim, T.-H., & Wei, H.-W. (2011). A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography, **Sensors**, Vol.11, No.5, pp.4767 - 4779.

Zhang, M., Gong, C., Feng, Y., & Li, C. (2008). Energy Predicted Shortest Routing Tree Algorithm In Wireless Sensor Networks, **Advances in Computation and Intelligence, Lecture Notes in Computer Science, LNCS,** Vol.5370, pp.117-124.

نظام توجيه آمن لشبكات الإستشعار اللاسلكية

إعداد

مها خالد سعاده

المشرف

الدكتورة إيمان المومني

ملخـــــــص

تعتبر شبكات الاستشعار اللاسلكية موضوعا مهما حيث حظيت مؤخرا باهتمام كبير في العديد من الأبحاث. ويأتي هذا الاهتمام من نجاح استخدام تكنولوجيا الاستشعار في العديد من التطبيقات المدنية والعسكرية والصناعية. تعتبر محدودية المصادر و خصائص الشبكات اللاسلكية من أهم التحديات التي تواجه تطوير ونشر بروتوكولات شبكات الإستشعار اللاسلكية. أي بروتوكول يتم إقتراحه لشبكات الإستشعار اللاسلكية يجب أن يراعي القدرات المنخفضة و المصادر المحدودة لهذه الشبكات.

لقد تم اقتراح العديد من بروتوكولات التوجيه لشبكات الاستشعار اللاسلكية. بعض هذه البروتوكولات تأخذ محدودية الطاقة لشبكة الاستشعار بعين الاعتبار في حين أن البعض الآخر لا ينظر الى طاقة الشبكة. في هذه الأطروحة سنعمل على تحسين كفاءة بروتوكول التوجيه من خلال تطبيق بعض الآليات الأمنية لبناء بروتوكول توجيه آمن ذو كفاءة في استخدام طاقة الشبكة و القدرة على حماية الشبكة من أنواع مختلفة من الهجمات الأمنية. الفكرة الرئيسية هي أن نقيم بروتوكول التوجيه قبل و بعد تفعيل التطبيقات الأمنية لمعرفة أثر المخترقين على هيكلية الشبكة و عملية التوجيه. بالاضافة الى قياس تكلفة تفعيل هذه التطبيقات الأمنية.

تم استخدام محاكي الشبكات QualNet لتقييم بروتوكول التوجيه و استخدام CBC-MAC و ECDSA كأمثلة على التطبيقات الأمنية. اظهرت النتائج أن النظر فقط لمحدودية الموارد لأجهزة الاستشعار ليست كافية لبناء بروتوكول توجيه فعال بدون حماية الشبكة من الهجمات المختلفة حيث أن الهجمات الأمنية على الشبكة تؤدي الى هبوط طاقة الشبكة مع الوقت.

بعد تفعيل التطبيقات الأمنية أظهرت النتائج أنه بغض النظر عن عدد المخترقين سيتم استبعادهم من الشبكة و نتيجة لذلك فإن هيكل الشبكة سيكون آمنا لنقل المعلومات. بالإضافة الى ذلك فإن النتائج أظهرت أن استخدام CBC-MAC يستهلك ٠,٠٠٠٦٤ % من طاقة الشبكة في حين أن استخدام ECDSA يستهلك ٠,٠٠٩١ % من الطاقة. بالرغم من أن اسخدام التطبيقات الأمنية يكلف الشبكة جزءا من طاقتها إلا أن عدم استخدامها قد يؤدي الى هجمات أمنية تكلف الشبكة ما يعادل ٤,٧ أضعاف ما يكلفه استخدام التطبيقات الأمنية.